Um estudo prático das ameças de segurança em dispositivos portáteis com Windows Mobile

Bruno Paulo Usiglio Kovacs e Vanesa de Freitas Monteiro
Departamento de Informática – PUC-Rio
Rua M. S. Vicente 225, 22453-900
Rio de Janeiro RJ, Brazil
{bruno.kovacs@gmail.com ; freitasmon@ig.com.br}

Professor orientador: Markus Endler

Resumo: esta monografia se propõe a apresentar ameaças de segurança a dispositivos de computação móvel, dando foco principal àqueles que utilizam o sistema operacional Windows Mobile. As vias de contaminação abordadas serão os padrões BlueTooth e Wi-fi (802.11). Experimentos práticos foram realizados, procurando reproduzir pesquisas de grupos especializados no assunto.

Palavras-chave: PDA, PocketPC, *handheld*, Wi-Fi, Bluetooth, redes sem-fio, malware, trojan, worm, ameaça, segurança, Windows Mobile, porta dos fundos, WEP, WPA, criptografia, chave.

Índice

1. Introdução 3
   1.1. Objetivo e Definições 4
   1.1.1. Definição de um dispositivo móvel 4
   1.1.2. Ameaça de segurança 4
   1.1.3. Rede sem fio 5
   1.2. Introdução ao Windows Mobile 5
   1.3. Introdução ao IEEE 802.11 6
   1.3.1. Funcionamento 8
   1.3.2. Origem e significado do termo 'Wi-Fi' 9
   1.4. Introdução ao WEP 9
   1.5. Introdução ao WPA 10
   1.6. Introdução ao Bluetooth 11
2. Ataque Locais 13
   2.1.1. Obstáculos encontrados para se atacar um PDA 13
   2.1.2. Arquivos .CAB 14
   2.1.3. Execução automática de aplicações (*auto-run*) 14
   2.1.4. Restauração das configurações de fábrica 15
   2.1.5. Internet Explorer para PDAs 16
   2.1.6. Visão reduzida de URLs 16
   2.1.7. Modelo de Objeto de Domínio do PIE (PIE Domain Object Model) 17
   2.1.8. Acesso a arquivos locais usando o Pocket IE 17
   2.1.9. Monitoração de teclas digitadas 18
   2.1.10. Análise forense 19
   2.1.11. Engenharia reversa de binários 19
   2.1.12. Servidor de FTP oculto 21
   2.1.13. Controle remoto 22
   2.2. Descrição de ameaças específicas 23
3. Ataques através da Rede 23
   3.1. Classificação geral de tipos de ataques 23
   3.1.1. Formas de ataques genéricas 23
   3.1.2. Quebra de chave da criptografia 24
   3.1.3. Tomada de controle do dispositivo 24
   3.1.4. Pontos de acesso falsos 24
   3.1.5. Visão geral de worms/virus conhecidos 25
   3.2. Ataques via interface Bluetooth 26
   3.2.1. Varrendo endereços Bluetooth 26
   3.2.2. Reduzindo a margem de endereços possíveis 27
   3.2.3. Descobrindo endereços Bluetooth enquanto se comunicam 27
   3.2.4. Comunicação via Bluetooth entre dispositivos & segurança 28
   3.2.5. Problemas relacionados a fabricantes 29
   3.2.6. O Risco de conexão à APs falsos 30
   3.2.7. Ataques específicos 32
   3.3. Ataques via interface IEEE 802.11 34
   3.3.1. Ataques ao WEP 34
   3.3.2. Ataques ao WPA 35
   3.3.3. Ataques de invasão de memória (Buffler Overflow attacks) 35
   3.3.4. Captura de tráfego 36
   3.3.5. Análise de vulnerabilidades 37
   3.3.6. Abrindo portas para um ataque 37
4. Checklist de Segurança para dispositivos móveis em redes sem-fio 38
5. Avaliação Prática 40
   5.1. Testes com Emuladores vs Teste com dispositivos físicos 40
   5.1.1. Descrição do ambiente de testes com emuladores 40

5.1.2. Descrição do ambiente de testes com dispositivos físicos 41
5.1.3. Vantagens e desvantagens quanto aos ambientes 42
5.2. Discussão sobre metodologia e critérios de avaliação 42
5.3. Testes com emuladores 43
5.4. Testes locais 45
5.5. Testes com Bluetooth 48
5.6. Testes com IEEE 802.11 50
6. Conclusão 53
7. Referências Bibliográficas 55

Índice de figuras

Figura 1: IEEE 802.11 e o modelo OSI/ISO 7
Figura 2: Opção de ser descoberto ou não 12
Figura 3: Código para retornar à configuração de fábrica do dispositivo (Hard reset) 15
Figura 4: Código em HTML que irá finalizar imediatamente o Pocket Internet Explorer 16
Figura 5: barra de endereços reduzida pode enganar usuários 17
Figura 6: servidor de FTP identifica-se através de ícone na área de trabalho 21
Figura 7: Janela exibida ao iniciar a aplicação VirtualCE 22
Figura 8: Exemplo de configuração da autenticação de uma configuração Bluetooth. 29
Figura 9: A descoberta de dispositivos não divulga seu endereço Bluetooth. 31
Figura 10: vxSniffer em ação 36
Figura 11: Emulação do Windows Mobile 2003 SE em PocketPC 41
Figura 12: Emulação do Windows Mobile 2003 SE em SmartPhone 41
Figura 13: VxSniffer coletou tráfego da interface local 44
Figura 14: Detalhes de uma requisição do protocolo ARP 44
Figura 15: Acesso via FTP através da Internet ao PocketPC e exibição dos arquivos locais. 46
Figura 16: Autenticação com senha para acesso remoto (Através da aplicação VirtualCE) 46
Figura 17: Controle remoto do PocketPC via Internet 46
Figura 18: Controle remoto do PocketPC via Internet 47
Figura 19: Controle remoto do PocketPC via Internet 47
Figura 20: Editando o registro do Windows Mobile através da aplicação “Mobile Registry Editor” 48
Figura 21: Habilitando a interface Bluetooth do dispositivo 49
Figura 22: Configurando a interface Bluetooth do dispositivo para estar visível 49
Figura 23: Aplicação btCrawler com função de bluesnarfing habilitada via edição de registro. 49
Figura 24: Mini-stumbler não reconheceu a interface de rede sem fio. 50
Figura 25: Captura de tráfego da rede 802.11 do LAC 51
Figura 26: Detalhes do segmento TCP capturado 51
Figura 27: Análise do conteúdo capturado. Pode-se visualizar o conteúdo das requisições. 52
Figura 28: Exibição dos pacotes capturados. 52
Figura 29: Ferramenta E-eye WiFi Scanner identificou uma rede 802.11 com WEP habilitado 53

1. Introdução

Um PDA (Personal Digital Assistant), ou Assistente Pessoal Digital, é um computador de dimensões reduzidas, dotado de grande capacidade computacional, normalmente cumprindo as funções de agenda, sistema de escritório, oferecendo recursos multimídia e entretenimento, com possibilidade de interconexão com um computador pessoal e uma rede sem-fio para acesso a correio eletrônico e internet.

Infelizmente, este simples dispositivo pode gerar um furo de segurança na estrutura de muitas corporações, que pode ser explorado por pessoas com fins "não amigáveis". Atualmente, a maioria das empresas nem mesmo cita a verificação de dispositivos móveis em suas políticas de segurança ou em sistemas de controle, ou ainda, não possuem idéia de como estes são utilizados na sua própria rede ou em localidades remotas. Não apenas o dispositivo móvel em si pode ser comprometido, tendo suas informações capturadas, mas pode ser contaminado por um cavalo de tróia e transformado em um livre ponto de acesso à rede corporativa.

Este documento analisa algumas das formas de se atacar um dispositivo móvel e quais as conseqüências que poderão ser geradas.

1.1. Objetivo e Definições

O objetivo principal deste trabalho é apresentar ameaças de segurança que podem afetar dispositivos de computação móvel, considerando o escopo dos sistemas operacionais de mercado Windows Mobile 2003/5.0 e as tecnologias de rede sem-fio Bluetooth e 802.11. Estas tecnologias serão apresentadas de forma introdutória, de modo a contextualizar as ameaças estudadas.

Além da teoria apresentada, experiências práticas são conduzidas, apresentando um relatório técnico com resultados obtidos no final do trabalho.

1.1.1. Definição de um dispositivo móvel

Vamos considerar que um dispositivo móvel é um equipamento digital que serve para realizar tarefas diárias de trabalho. Isso inclui todos os Pocket PCs, Palms, SmartPhones e relacionados. Além destes, outros dispositivos móveis que utilizam a plataforma Windows CE.NET. Apesar de laptops se enquadrarem neste perfil, estes não terão foco deste trabalho.

1.1.2. Ameaça de segurança

São consideradas ameaças de segurança, aquelas que possam comprometer a confidencialidade, integridade e disponibilidade de dados e serviços utilizados pelos usuários da

infra-estrutura de computação móvel. A seguir, definimos cada um dos três pilares da segurança de informação:

Confidencialidade - propriedade que limita o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

Integridade - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).

Disponibilidade - propriedade que garante que a informação esteja sempre disponívei para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

1.1.3. Rede sem fio

Rede sem fio é um termo utilizado para designar a interconexão de computadores em um sistema sem o uso de fios, por meio de dispositivos apropriados. Atualmente, as ondas de rádio são o meio mais eficaz para possibilitar estas ligações. São exemplos de tecnologias de rede sem fio abordadas neste artigo o BlueTooth e o 802.11, vulgo Wi-fi.

1.2. Introdução ao Windows Mobile

Visão Geral

O Microsoft Windows Mobile é uma plataforma de sistema operacional de 32 bits, multitarefa e multisegmentado. Tem uma estrutura de arquitetura aberta que dá suporte a uma variedade de dispositivos de comunicação, entretenimento e computação móvel. É um sistema operacional inteiramente novo, compacto, portátil e proporciona uma interface intuitiva e de fácil aprendizado, incorporada de elementos familiares do Windows para PCs. É compatível com os melhores e mais úteis hardwares do mercado tais como: modem cards, Flash cards, Color Digital Camera Card, cabos de saída VGA e porta Paralela, entre outros.

Diferentes Versões

O Windows Mobile, lançado em Junho de 2003, está disponível em diferentes classes de equipamentos:

Windows Mobile Pocket PC

Permite controlar os contatos, agenda, tarefas a fazer, anotações, tocar músicas, vídeos, jogar, receber e enviar e-mails, e mensagem instantânea, dentre outras funções. Essa é a versão do Widows Mobile para os computadores móveis.

Windows Mobile Pocket PC Phone

O sistema combina os recursos padrões do Windows Mobile para Pocket PC com os recursos para telefonia, integrados ao PDA. É possível, por exemplo, discar para uma pessoa em sua lista de contatos, enviar mensagens SMS, navegar pela Internet, etc. Pode-se considerar esse sistema o Pocket PC com recursos de celular, onde o principal continua sendo o PDA;

Windows Mobile Smartphone

Neste caso o foco é diferente. O Windows Mobile para Smartphones integra recursos de PDA em um equipamento criado para ligações de voz, e do tamanho dos atuais aparelhos celulares. O sistema é desenvolvido para operação com uma mão, e otimizado para comunicação de voz e dados, permitindo o acesso sem fio ao Outlook, navegação segura na Internet e rede corporativa. Em função das diferenças em relação às outras versões do Windows Mobile, os programas para smartphone são específicos, e no geral incompatíveis com as outras versões do sistema.

1.3. Introdução ao IEEE 802.11

Uma rede sem fio do padrão 802.11 (wireless LAN - WLAN ou WiFi) é um sistema de transmissão de dados desenvolvido para oferecer acesso à rede independentemente de localização, através de ondas de rádio ao invés de uma infra-estrutura cabeada.

A aceitação em larga escala desta tecnologia depende da criação de um padrão de mercado para garantir a compatibilidade e confiabilidade de produtos de diversos fabriacantes.

A especificação 802.11 [Padrão IEEE 802.11 (ISO/IEC 8802-11: 1999)] como um padrão para redes sem fio foi formalmente aprovada pelo Instituo de Engenheiros de Elétrica e Eletrônica (Institute of Electrical and Electronics Engineers - IEEE) no ano de 1997. Esta versão do 802.11 oferece velocidades de transmissão de dados de 1 e 2 Mbps e um conjunto de métodos de sinalização e outros serviços. Como todos os padrões do IEEE, o 802.11 tem foco nas duas camadas inferiores do modelo OSI/ISO: camadas física e de enlace. Qualquer aplicação de rede, sistema operacional de rede, protocolo, incluindo o TCP/IP e o Novell Netware, irão funcionar em

redes sem fio em conformidade com este padrão da mesma forma que funcionam nas redes Ethernet.

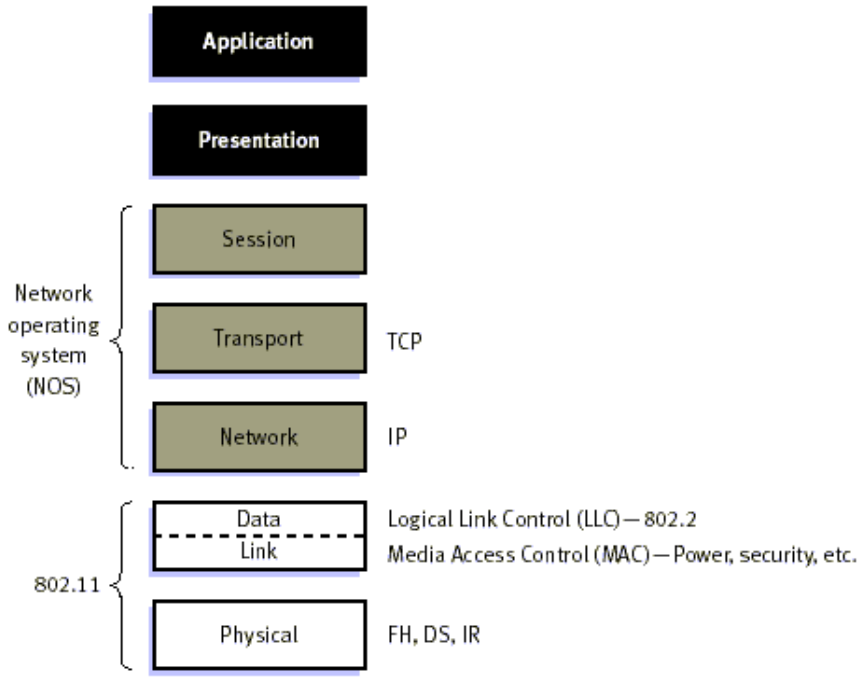


Figura 1: IEEE 802.11 e o modelo OSI/ISO

A grande motivação e benefício quanto às redes sem fio é o aumento de mobilidade. O fato da estação não estar confinada a um ponto de rede cabeado, permite ao usuário que se locomova livremente por praticamente qualquer lugar, conectado à rede.

Outra vantagem é o custo-benefício da implantação de uma rede que exija conectividade em localidades de difícil acesso para realizar cabeamento, como no caso de prédios antigos e paredes rígidas. Além disso, a redução de custo total de propriedade, especialmente em lugares de mudanças constantes, devido ao mínimo de cabeamento realizado e baixo custo de instação de equipamentos e pontos de acesso para usuários.

Redes sem fio permitem usuários acessar recursos da rede sem que dependam de pontos de rede em lugares específicos, dando assim as seguintes vantagens:

- Acesso imediato a informações de pacientes médicos, ao lado dos mesmos, o que é útil para médicos e para equipes médicas.
- Acesso rápido para consultores externos ou auditores, que estejam em serviço ao longo da extensão da empresa.

- Facilita o controle de supervisores como gerentes de linhas de montagem, auditors de depósitos ou engenheiros de construção, pois por exemplo oferece acesso a bancos de dados de qualquer lugar.
- Configuração de rede simplificada, exigindo menor dependência do envolvimento de times de suporte em eventos exporádicos, como palestras.
- Acesso mais rápido a informações de clients para vendedores e varejistas, resultando em uma melhor qualidade de serviço e consequente satisfação do cliente.
- Permite administradores de rede acessarem recursos a partir de qualquer lugar dentro da empresa, permitindo-os resolver problemas com mais velocidade.

O padrão 802.11 possui 6 versões de modulação pelo ar, todas usando o mesmo protocolo. As mais populares são as versões 'a' , 'b' e 'g'. Estas, foram desenvolvidas levando em consideração problemas de segurança, mas a versão que teve este assunto levado mais à sério foi a versão 'i'. Outras versões do padrão (c–f, h, j) são melhoramentos e extensões de versões anteriores. O 802.11b foi o primeiro padrão largamente aceito, seguido pelas versões 802.11a e 802.11g.

Os padrões 802.11b e 802.11g usam a faixa de freqüência de 2.4 gigahertz (GHz) e devido a este fato, podem sofrer interferências com fornos de micro-onda, telefones sem-fio, dispositivos Bluetooth e outros equipamentos que fazem uso da mesma faixa. O 802.11a usa a faixa de 5 GHz, e por isso não é afetado por produtos que operem na faixa de 2.4Ghz.

A faixa de freqüência do spectro utilizada pode ser utilizada em vários países, sendo que as limitações mais acirradas ocorrem nos Estados Unidos.

1.3.1. Funcionamento

Uma típica rede Wi-Fi contem um ou mais pontos de acesso (Access Points - APs) e um ou mais clientes. Um AP transmite para todos que podem escutar (*broadcast*) o seu SSID (Service Set Identifier, nome da rede) através de pacotes chamados beacons, o que acontece normalmente a cada 100 ms. Os beacons são transmitidos na velocida de 1 Mbit/s, são pacotes que tem pouca duração e por isso não impactam significativamente em performance. Como a velocidade mínima aceitável para se conectar à rede é de 1Mbit/s, assume-se que a taxa de transmissão dos beacons é suficiente para atender até o cliente em piores situações.

Baseado no SSID, o cliente pode escolher à qual rede se conectar. Caso mais de um AP pertença à mesma rede, o firmware do cliente pode escolher automaticamente o AP mais próximo. Como a transmissão é feita através do ar neste tipo de rede, as mesmas propriedades de uma rede em barra são compartilhadas, por exemplo, até colisões podem aparecer. No entanto, as redes Wi-Fi não são capazes de realizar detecção de colisão, e por isso usam um método para evitar colisões.

1.3.2. Origem e significado do termo 'Wi-Fi'

Apesar da similaridade entre os termos 'Wi-Fi' e 'Hi-Fi', declarações feitas por Phil Belanger, membro do grupo Wi-Fi Alliance contradizem a crença popular de que 'Wi-Fi' significa 'Wireless Fidelity.'

De acordo com Belanger, a empresa Interbrand desenvolveu a marca 'Wi-Fi' para o grupo Wi-Fi Alliance para ser usada para descrever produtos de rede sem fio baseados no padrão IEEE 802.11. Segundo Belanger, o termo 'Wi-Fi' e seu logotipo similar a um yin yang foram criados pela Interbrand, contratada pelo grupo para identificar produtos compatíveis e fazer uma campanha de marketing.

1.4. Introdução ao WEP

O primeiro protocolo de segurança adotado, que conferia no nível do enlace uma certa segurança para as redes sem fio foi o WEP (Wired Equivalent Privacy).

Este protocolo, usado ainda hoje, utiliza o algoritmo RC4 para criptografar pacotes que são trocados numa rede sem fio a fim de tentar garantir confidenciabilidade aos dados de cada usuário. Além disso, utiliza-se também a CRC-32, uma função de detecção de erros que ao fazer o "checksum" de uma mensagem enviada gera um ICV (Integrity Check Value) que deve ser conferido pelo receptor da mensagem no intuito de verificar se a mensagem recebida foi corrompida e/ou alterada no meio do caminho.

Vulnerabilidades do WEP

No entanto, após vários estudos e testes realizados com este protocolo, foram achadas algumas vulnerabilidades e falhas que fizeram com que o WEP perdesse quase toda a sua credibilidade.

No WEP, os dois parâmetros que servem de entrada para o algoritmo RC4 são a chave secreta k de 40 bits ou 104 bits e um vetor de inicialização de 24 bits. A partir desses dois parâmetros, o algoritmo gera uma seqüência criptografada RC4 (k,v).

Porém, como no WEP a chave secreta k é a mesma utilizada por todos os usuários de uma mesma rede, devemos ter um vetor de inicialização diferente para cada pacote a fim de evitar a repetição de uma mesma seqüência RC4. Essa repetição de seqüência é extremamente indesejável, pois dá margem a ataques bem sucedidos e conseqüente descoberta de pacotes por eventuais intrusos.

Além disso, há também uma forte recomendação para que seja feita a troca das chaves secretas periodicamente aumentando-se com isso a segurança da rede. Porém, essa troca quando

é feita, é realizada manualmente de maneira pouco prática e por vezes inviável, quando se trata de redes com um número muito alto de usuários.

Ainda, uma falha do WEP constatada e provada através de ataques bem sucedidos é a natureza de sua função detectora de erros. A CRC-32 é uma função linear e que não possui chave. Essas duas características tornam o protocolo suscetível a dois tipos de ataques prejudiciais e indesejáveis: é possível fazer uma modificação de mensagens que eventualmente tenham sido capturadas no meio do caminho sem que isso seja descoberto pelo receptor final devido a linearidade da função detectora de erros, e além disso, pelo fato da função não possuir uma chave, é também possível descobrir uma seqüência secreta RC4 e de posse desta, ser autenticado na rede e introduzir mensagens clandestinas nesta.

1.5. Introdução ao WPA

Também chamado de WEP2, ou TKIP (Temporal Key Integrity Protocol), a primeira versão do WPA (Wi-Fi Protected Access) surgiu de um esforço conjunto de membros da Wi-Fi Aliança e de membros do IEEE, empenhados em aumentar o nível de segurança das redes sem fio ainda no ano de 2003, combatendo algumas das vulnerabilidades do WEP.

A partir desse esforço, pretendia-se colocar no mercado produtos que utilizassem WPA, pois algumas características fazem dele uma ótima opção de segurança:

- Pode-se utilizar WPA numa rede híbrida que tenha WEP instalado.
- Migrar para WPA requer somente atualização de software.
- WPA é desenhado para ser compatível com o próximo padrão IEEE 802.11i.

Vantagens do WPA sobre o WEP

A substituição do WEP pelo WPA trouxe como vantagem uma melhora da criptografia dos dados ao utilizar um protocolo de chave temporária (TKIP) que possibilita a criação de chaves por pacotes, além de possuir função detectora de erros chamada Michael, um vetor de inicialização de 48 bits (ao invés de 24 como no WEP) e um mecanismo de distribuição de chaves.

Além disso, uma outra vantagem é a melhoria no processo de autenticação de usuários. Essa autenticação utiliza o 802.1x e o EAP (Extensible Authentication Protocol), que através de um servidor de autenticação central faz a autenticação de cada usuário antes deste ter acesso a rede.

O WPA, que está em fase de substituição do WEP, conta com tecnologia aprimorada de criptografia e de autenticação de usuário. Cada usuário tem uma senha exclusiva, que deve ser digitada no momento da ativação do WPA. No decorrer da sessão, a chave de criptografia será

trocada periodicamente e de forma automática. Assim, torna-se infinitamente mais difícil que um usuário não-autorizado consiga se conectar à rede sem fio.

A chave de criptografia dinâmica é uma das principais diferenças do WPA em relação ao WEP, que utiliza a mesma chave repetidamente. Esta característica do WPA também é conveniente porque não exige que se digite manualmente as chaves de criptografia - ao contrário do WEP.

1.6. Introdução ao Bluetooth

A tecnologia de rede sem fio Bluetooth oferece uma maneira simples para realizar a comunicações de diversos dispositivos móveis entre si, e também o acesso destes à Internet sem a necessidade de cabos.

O Bluetooth foi construído para facilitar a transmissão de informação dentro de uma faixa relativamente pequena (em torno de dez metros). Trabalha de forma a reduzir o risco de interferências entre dispositivos Bluetooth. Mudando a freqüência 1600 vezes em um segundo, é muito improvável que dois dispositivos, numa mesma área, terão conflito entre si.

O que torna o Bluetooth realmente atraente é que ele automaticamente controla o processo de comunicação entre dispositivos. Varrendo a área em volta por outros dispositivos Bluetooth e, estabelecendo uma conexão entre os descobertos, é criado um tipo de mensagem informando a existência da rede Bluetooth, denominada piconet, que se propaga entre os dispositivos criando uma rede de comunicação.

O Bluetooth é suportado e utilizado em produtos de mais de 3000 empresas, tais como Sony Ericsson [10], Nokia [27], Motorola [11], Intel [13], IBM [14], Toshiba [15], Apple [21], Microsoft [16] e até mesmo a Toyota [17], Lexus [19] e BMW [18]. Uma variedade de produtos disponíveis no mercado possuem rádios Bluetooth integrados, como por exemplo impressoras, computadores portáteis, teclados, carros e os mais populares, telefones celulares, tomando 60% do mercado de dispositivos Bluetooth. Esta tecnologia já ganhou muita popularidade, com mais de 3 milhões de produtos sendo vendidos toda semana. De acordo com o IDC [28], haverá mais de 922 milhões de dispositivos com Bluetooth em todo o mundo até 2008. A tecnologia pode ser bastante interessante e útil, mas também pode ser uma grande ameaça à privacidade de seus usuários.

A tecnologia foi padronizada por um grupo chamado "Blueetooth Special Interest Group (SIG)". As empresas fundadoras do grupo são a Ericsson [20], IBM [14], Intel [13], Nokia [27] e Toshiba [15], e depois, passaram a fazer parte 3Com [24], Lucent Technologies [25], Microsoft Corporation [16] e Motorola Inc [11].

A tecnologia ganhou sua versão atual, que trabalha com uma faixa de freqüência disponível globalmente de 2.4 GHz, que permite que dois dispositivos móveis, em um raio de

distância de 10-100 metros, transfiram/recebam dados com velocidade de 723.2Kbps ou 2.1Mbps utilizando uma nova especificação de transferência de dados licenciada em 2005 (Enhanced Data Rate specification). Cada dispositivo pode simultaneamente se comunicar com até sete outros dispositivos.

O Bluetooth foi feito pensando-se em segurança, oferecendo serviços como autenticação, criptografia, qualidade de serviço e outros recursos de segurança. No entanto, a tecnologia ainda está vulnerável em vários aspectos, abrindo portas para ataques.

Os usos mais comuns do Bluetooth atualmente são:

- Fone de ouvido para celular sem fio
- Sincronizar informações como calendários, agenda telefônica, entre um PDA e um PC
- Conectar uma impressora, teclado, ou mouse a um PC sem uso de fios
- Realizar transferência de fotos ou músicas entre telefones celulares

A tecnologia está em constante evolução, visando aumentar seu grau de segurança, funcionalidade e facilidade de uso.

Recursos de segurança da tecnologia Bluetooth

O recurso mais comum e mais conhecido de um dispositivo Bluetooth é a possibilidade de mantê-lo invisível ou não, perante outros ao seu redor, como mostrado a seguir:

Figura 2: Opção de ser descoberto ou não

Quando um dispositivo está visível, este pode ser facilmente encontrado utilizando scanners (programas de varredura da rede sem fio em busca de dispositivos). Alguns scanners também têm a função de *sniffer*, ou seja, podem fazer a coleta de tráfego de forma passiva.

Configurar o dispositivo como invisível, impede que scanners o encontrem, mas não impede que dispositivos que tenham conhecimento do endereço físico de sua interface de rede (MAC) realizem comunicação com este, por exemplo, quando os dispositivos já estavam se comunicando previamente.

2. Ataque Locais

Ataques locais são aqueles que se faz necessário a manipulação direta do dispositivo móvel, ou seja, deve-se tê-lo nas próprias mãos para executar a operação desejada. Nesta seção, serão apresentadas diversas técnicas de ataque realizadas nesta modalidade, objetivando principalmente o roubo de informações, infecção do dispositivo para posterior entrada através de redes sem fio e mostrar o quanto se torna vulnerável o dispositivo quando em mãos erradas.

2.1.1. Obstáculos encontrados para se atacar um PDA

Um dos obstáculos que um atacante deverá atravessar é o fato de que a maioria dos sistemas operacionais de dispositivos móveis estão armazenados em memória somente para leitura (ROM). Este é um grande desafio, pois realizar a depuração de aplicações que são executadas diretamente na ROM nem sempre é possível. Como resultado, o atacante deverá direcionar o seu ataque para uma aplicação terceira, que tenha sido instalada manualmente pelo dono do sistema. Assim, deve-se buscar uma falha nesta aplicação através de uma técnica conhecida como "teste cego" (*blind testing* ou *blackbox testing*), pois não se tem acesso ao código desta, mas pode-se tentar atacá-la "por fora", por exemplo, através de campos de entrada de variáveis.

Em segundo lugar, pode-se dizer que cada PDA é único. Isso significa que se a Dell [22] e a HP [23] oferecem modelos portando Windows Mobile, não significa que estes usam a mesma versão do sistema. Cada empresa instala junto com os módulos essenciais do sistema, componentes particulares, o que pode dificultar bastante o desenvolvimento de código malicioso para tais equipamentos. Como se já não fosse suficiente, atualizações da ROM podem impactar drasticamente no sistema de arquivos utilizado e como os módulos de sistema mais básicos são carregados. Como resultado, existem grandes diferenças entre dois PDAs com relação ao endereçamento de memória.

Em terceiro, as técnicas de ataque a dispositivos móveis são relativamente novas. Um atacante deve ter dedicação e grande conhecimento tanto do processador quanto do sistema operacional do alvo. O ponto em que queremos chegar é: atacar um PDA não é tão fácil quanto atacar um PC.

Uma vez aceitas as limitações, iremos apresentar os vetores e métodos usados para deixar um PDA pronto para ser atacado.

2.1.2. Arquivos .CAB

Arquivos .CAB (*cabinet* files) são usados pela Microsoft [16] há muitos anos para agrupar diversos arquivos em um único, que serão usados durante a instalação de alguma aplicação. Desta forma, não é nenhuma surpresa que o mesmo formato de arquivo.CAB é usado pelo Windows Mobile para instalar programas que foram tanto transferidos diretamente para o PDA pela rede, quanto transferidos através de uma conexão do ActiveSync*. O problema não está no fato do PDA usar estes arquivos, mas sim em como estes são processados e sequencialmente excluídos.

Próximo à criação dos arquivos .CAB, foi descoberto que tais arquivos se auto-excluíam após terem sido executados. Enquanto este comportamento é provavelmente uma tentativa de ajudar usuários a manterem a memória de seus dispositivos limpa, ironicamente se parece muito com o de cavalos de tróia encontrados em PCs. O comportamento em si observado não aparenta um risco de segurança significativo, porém é uma boa forma de ser ocultar a instalação de portas de entrada em PDAs. Como a execução de .CABs pode criar arquivos e entradas no registro do sistema, além de substituir ou excluir outros existentes, um usuário pode ser facilmente induzido a instalar código malicioso escondido em um pacote aparentemente inofensivo. Por exemplo, como saber se o jogo que foi transferido de um site na Internet não contém surpresas indesejáveis? A boa notícia é que o Windows Mobile não exclui automaticamente os arquivos .CAB. Esta medida não irá proteger o sistema contra infecção, mas irá possibilitar a inspeção do conteúdo dos arquivos instalados.

2.1.3. Execução automática de aplicações (*auto-run*)

Outra grande ameaça é a execução automática de aplicações. A simples inserção de cartões de memória pode levar à execução de código malicioso. Como o Windows Mobile foi desenvolvido pela Microsoft, a presença de um arquivo chamado “autorun.exe” em uma pasta chamada “2577” (considerando que o dispositivo trabalha com processador ARM) será copiado para a pasta local do Windows e executado. Se o arquivo for algum tipo de código malicioso, será executado sem a intervenção do usuário. Para ilustrar o estrago potencial, imagine que o cavalo de tróia “brador.exe” (detalhado mais adiante), fosse renomeado para “autorun.exe” e inserido nesta pasta, dentro de um cartão de memória dedicado a jogos de Atari. O cartão provavelmente

seria compartilhado entre muitas pessoas dentro de uma empresa e infectaria cada PDA sem o consentimento de seus donos. O estrago causado na verdade vai de acordo com a vontade do desenvolvedor do cavalo de tróia, que pode variar desde a instalação de um servidor FTP oculto até a execução de um mecanismo do dispositivo que apaga todos os dados, voltando à sua configuração original (*hard reset*).

2.1.4. Restauração das configurações de fábrica

Os PDAs em geral armazenam seus dados em memória interna dos tipos RAM e ROM. Os componentes básicos do sistema operacional são gravados em memória Flash, enquanto os arquivos e programas adicionais em memória RAM. Os modelos mais recentes começaram a incluir maior quantidade de memória ROM, mas mesmo assim não é onde a maioria dos documentos, calendários e listas de afazeres são armazenados.

O efeito colateral resultante desta arquitetura é o fato de que o equipamento precisa de uma fonte constante de energia, caso contrário, irá perder as informações gravadas na RAM. A maioria das pessoas está ciente das conseqüências de se deixar a bateria descarregar completamente, mas o que as pessoas não tem conhecimento é que a limpa total dos dados pode ser facilmente causada com a execução de apenas algumas linhas de código, apresentadas a seguir. Caso aconteça destas linhas de código serem executadas acidentalmente através da inserção de um cartão de memória ou através de um executável transferido pela Internet, o PDA voltará ao estado em que foi tirado de sua caixa.

```
#include <windows.h>
#include <winioctl.h>
#define IOCTL_HAL_REBOOT CTL_CODE(FILE_DEVICE_HAL, 15, METHOD_BUFFERED,
FILE_ANY_ACCESS)

extern "C" __declspec(dllimport)void SetCleanRebootFlag(void);
extern "C" __declspec(dllimport) BOOL KernelIoControl(
DWORD dwIoControlCode,
LPVOID lpInBuf,
DWORD nInBufSize,
LPVOID lpOutBuf,
DWORD nOutBufSize,
LPDWORD lpBytesReturned);
int WINAPI WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance,
LPTSTR lpCmdLine, int nCmdShow)
{
SetCleanRebootFlag();
KernelIoControl(IOCTL_HAL_REBOOT, NULL, 0, NULL, 0, NULL);
return 0;
}
```

Figura 3: Código para retornar à configuração de fábrica do dispositivo (Hard reset)

O problema em si não é a existência deste código, mas sim o fato de que o comando "KernelIoControl" pode ser chamado por qualquer aplicação executando no sistema. Em outras

palavras, a falta de segurança no nível do núcleo do sistema operacional (*Kernel*), pode transformar um comando útil em um potencial ataque.

2.1.5. Internet Explorer para PDAs

No mundo dos PCs, o Internet Explorer é alvo de muitas aplicações contendo código malicioso que desejam explorar vulnerabilidades de segurança neste software (*exploits*). Felizmente, muitos destes ataques não são possíveis contra Pocket PCs porque o Pocket Internet Explorer (Pocket IE) é uma versão muito mais simples quando comparado a seu "pai". No entanto, este fato não significa que o PIE está livre de potenciais ataques. A seguir, descrevemos uma série de métodos que podem ser usados para atacá-lo:

Negação de serviço (DoS – Denial of Service)

Apesar do PIE portar uma versão também simplificada do interpretador de JavaScript, ainda é possível criar uma certa quantidade de ataques baseados em scripts que irão forçar o usuário a reiniciar seu PDA. Além destes, existem outros problemas que podem causar a finalização imediata do PIE. Por exemplo, uma das falhas do software existe na maneira em que ele verifica listas em HTML que usam formatação CSS (*Cascading Style Sheets*), ilustrado a seguir:

```
<style>
#layer1 div.sublayer1 { width:50%; margin:0 1 2 3; padding:4;
float:right; }
#layer1 div.sublayer2 { width:50%; margin:0 1 2 3; padding:4;
float:right; }
</style>
<div id="layer1">
<div class="sublayer1">
<ul>111</ul>
</div>
<div class="sublayer2">
<ul>222</ul>
</div>
</div>
```

Figura 4: Código em HTML que irá finalizar imediatamente o Pocket Internet Explorer

2.1.6. Visão reduzida de URLs

Há muitos anos atrás, foi descoberto que o Internet Explorer processava endereços contendo caracteres codificados com Unicode. Quando esta falha era combinada com requisições HTTP do tipo "usuario:senha@dominio", era possível enganar pessoas fazendo-as achar que estavam acessando links válidos. No entanto, estas eram direcionadas a páginas falsas. Dado o tamanho limitado da barra de endereços do PIE, é fácil imaginar que alguém não iria suspeitar

que foi vítima deste tipo de ataque. Por exemplo, o link a seguir irá direcioná-lo a www.airscanner.com, ao invés de www.puc-rio.br.

```
http://www.puc-rio.br&login.rand-
%00%01AE67D12EF9090AB933@%36%39%2E%30%2E%32%30%30%2E%31%30%36/
```

2.1.7. Modelo de Objeto de Domínio do PIE (PIE Domain Object Model)

Janelas e divisões (*frames*) sempre foram muito usadas por desenvolvedores de aplicações web para apresentar diversas páginas em um mesmo contexto de visualização. O ponto que gostaríamos de ressaltar é que o código presente em uma janela não pode enxergar ou modificar o código presente em outra. A razão para isso é que um atacante poderia esconder uma janela com código malicioso e tentar induzir o usuário e fornecer informações confidenciais. A seguir, ilustramos uma maneira de explorar este tipo de situação:

Note que a URL que aparentemente está sendo acessada (johnny.ihackstuff.com) está na verdade apontando para uma página em outro servidor Web. Quando acessada, o conteúdo da página é alterado pelo código não exibido devido ao pequeno tamanho da barra:

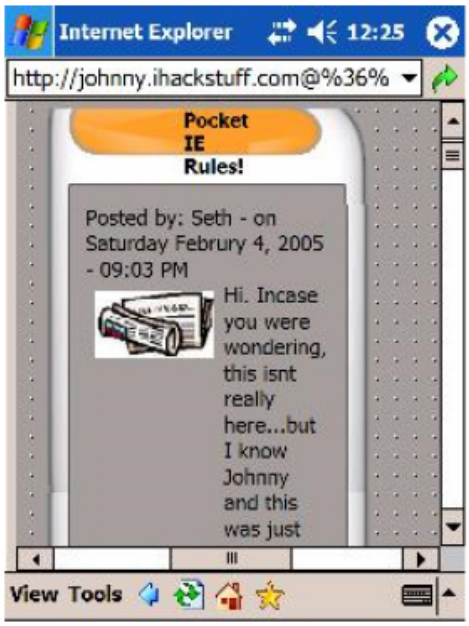


Figura 5: barra de endereços reduzida pode enganar usuários

2.1.8. Acesso a arquivos locais usando o Pocket IE

Outro recurso é a possibilidade de acesso a arquivos locais usando o Pocket Internet Explorer. Combinando este "artifício" com o problema citado anteriormente de execução de

código em frames ocultas, temos um verdadeiro risco de segurança. A seguir, listamos apenas uma pequena quantidade de tipos de arquivos que podem ser carregados através de um frame e aberto com o PIE:

- XLS
- HTC, HTP
- CPL (itens do painel de controle)
- INI
- Imagens 2BP
- Acesso à qualquer pasta
- Acesso à pasta raiz

Um vetor potencial encontrado é o fato do PIE permitir a visualização de páginas previamente acessadas, armazenadas em cache, e que podem ser posteriormente modificadas devido à uma frame oculta. Por exemplo, seria fácil obter o cache de acesso à página da PUC-RIO, alterar o código no que diz respeito às propriedades de formulários, direcionando o envio das informações preenchidas para um servidor web nocivo, o que iria capturar usuários e senhas quando o botão "Enviar" fosse pressionado.

2.1.9. Monitoração de teclas digitadas

O mundo dos PCs já está alerta quanto à infecção de leitores de teclado (*keyloggers*), pois há tempo são usados em ataques. No entanto, quando voltamos ao mundo dos Pocket PCs, não se tem dado a mesma importância ou considerado que a probabilidade de existência deste tipo de malware também existe. Provavelmente, pois o conceito de teclado em um dispositivo móvel é bem diferente do existente em PCs.

Ao invés de um dispositivo físico, o Pocket PC usa uma interface virtual que simula teclas reais. Mesmo que isso dificulte a captura de teclas digitadas, de jeito nenhum isso se tornou impossível. Quando o PDA é iniciado, primeiro ele avalia o registro do sistema e busca quaisquer dispositivos de entrada. Por padrão, são eles: o teclado, o "Block Recognizer", "Letter Recognizer" e o "Transcriber". Cada um destes é controlado por uma biblioteca dinâmica (DLL) presente em memória ROM, que possui tanto a interface gráfica quanto o código de conversão da entrada para caracteres. Por exemplo, o teclado principal é controlado pela biblioteca MSIM.DLL.

Graças à arquitetura dos painéis de entrada, é relativamente fácil criar um novo teclado e instalá-lo no sistema. Na verdade, existem diversas versões de teclado que podem ser obtidas e incorporadas ao sistema. Com base nisso, pode-se criar uma versão "especial" de teclado, com uma pitada adicional de código, que captura a entrada digitada e armazena-a em um arquivo texto. Depois disso, descobrimos quais seriam as entradas de registro necessárias para removermos a ligação com o teclado atual e as substituírmos por outras que chamarão o novo

teclado. Para finalizar, criamos um pacote .CAB contendo todas as nossas invenções; quando executado, substitui o teclado original por um idêntico, porém registrando cada tecla digitada.

A seguir, listamos as chaves de registro a serem alteradas para que a infecção seja bem sucedida:

1. IsSIPInputMethod desabilitada para o teclado original:
   CLSID: 42429667-ae04-11d0-a4f8-00aa00a749b9 (Trocar de 1 para 0)
2. Nome e ícone "Keyboard" carregado da dll keylogger.dll
3. Novo teclado possui possui o próprio CLSID configurado
4. HKCU\ControlPanel\SIP\DefaultIM\{CLSID}
5. IsSIPInputMethod habilitado para o teclado falso

Uma vez instalado, o usuário final não terá idéia de que seu teclado foi substituído por um modelo mais "avançado". Além disso, a única maneira de se descobrir que uma nova DLL está sendo chamada pelo sistema é através de depuração dos executáveis responsáveis pela gerência do teclado ou outro periférico usado pelo PDA.

2.1.10. Análise forense

Os PDAs em geral possuem uma capacidade de armazenamento de dados muito limitada (excluindo os cartões de memória que podem chegar a alguns GBs). Desta forma, se há necessidade de acesso realmente rápido, deve-se transferir estes dados a um PC. Ou então, faz-se uso de uma poderosa ferramenta de análise forense, isto é, uma ferramenta de visualização exata dos dados presentes na RAM e na ROM (*dumper*).

A comunidade policial começou recentemente a levar em conta PDAs encontrados em cenas de crime. Para ajudar, foram criados diversos programas de análise forense que podem encurtar o caminho de busca por informações interessantes. Por exemplo, a empresa ***Paraben*** [29] criou um software que instala um agente temporário em um PDA, que automaticamente transfere todo o conteúdo do mesmo para um PC, mantendo a integridade de ambos. Outras ferramentas fazem uso do recurso de execução automática mencionado anteriormente, carregando todo o conteúdo do PDA para um cartão de memória SD (*Secure Digital Card*) fazendo uso do recurso de *autorun*.

Isso significa que basta um período curto de tempo em mãos erradas para todos os dados de um PDA serem roubados.

2.1.11. Engenharia reversa de binários

A plataforma Windows Mobile para Pocket PCs é tipicamente executada sob um processador ARM (*Advanced RISC Multiprocessor*), conhecido por baixo aquecimento, por operar em baixo nível de potência e consumo de energia. Este fato, combinado com o reduzido número de instruções disponíveis (*RISC – Reduced Instruction Set*) faz com que aprender e entender o

conjunto de instruções seja relativamente fácil, principlamente quando comparado a outros processadores.

A primeira coisa que deve ser entendida ao se aplicar engenharia reversa a um arquivo binário é como o seu processador funciona. Em geral, este irá ler os códigos de operação (*opcodes*) em algum lugar específico na memória (indicado pelo registrador PC – *program counter*), e executar um comando bastante específico. Dependendo da instrução, o processador irá somar, subtrair, saltar para outra parte da memória ou simplesmente não fazer nada (NOP). Para ajudar o trabalho do processador, existem 32 registradores de 1 *byte* cada, totalizando 8 *bytes* de memória auxiliar. Tais registradores têm apenas a função de agilizar o trabalho do processador, pois o acesso a estes registradores é muito rápido, ao contrário do que acontece quando o acesso é realizado na RAM.

Para realmente explorar os binários de um PocketPC, serão necessários alguns programas. Primeiro, um desassemblador (*disassembler*) para converter o código hexadecimal para um formato mais legível, formado por instruções de operação (*opcodes*). Um bom exemplo deste tipo de aplicação é o "*IDA Pro*", o qual suporta binários do Windows CE. Em segundo, usamos o depurador de código incluído no conjunto de ferramentas de desenvolvimento para Windows CE da Microsoft (CE++). Este último é necessário para observar e alterar o código do binário em tempo de execução. Por último, será necessário um editor hexadecimal para alterar o código para realização de testes no sistema. A ferramenta sugerida é a "*UltraEdit*", mas existem diversas opções.

Tendo estas ferramentas reunidas, pode-se "passear" pelo Windows Mobile, observando cuidadosamente o que está acontecendo. A única coisa que resta nesta estória é a necessidade de se entender as instruções realizadas pelo processador. Em outras palavras, é de muita utilidade entender o assembly do ARM. Felizmente, entendendo as seguintes intruções, é possível ler e até mesmo escrever rotinas em assembly que poderão ser executadas em um Pocket PC:

- MOV (Mover) – Copia o valor de um registrador para outro, podendo ser o destino da cópia um registrador fixo (*hardcoded*) ou não.

- CMP (Comparar) – Compara o valor de um registrador com outro.

- B (Branch) – altera o fluxo de execução do programa, apontando para outro endereço de memória

- BL (Branch Link) - altera o fluxo de execução do programa, apontando para outro endereço de memória e depois retorna para posição inicial.

- LDR/STR (Load Register / Store Register) – Armazena ou carrega um dado para ou da RAM em um dos registradores.

Existem outros *opcodes* não mencionados aqui. Para maiores informações quanto ao assembly de processadores ARM, sugerimos uma visita à "www.arm.com" e a pesquisa nos manuais dos processadores.

2.1.12. Servidor de FTP oculto

Uma vez entendido como funciona um programa em baixo nível, pode-se fazer qualquer coisa para alterar as suas funcionalidades. Neste caso, foi possível transformar um legítimo servidor FTP em uma porta de entrada invisível e indetectável.

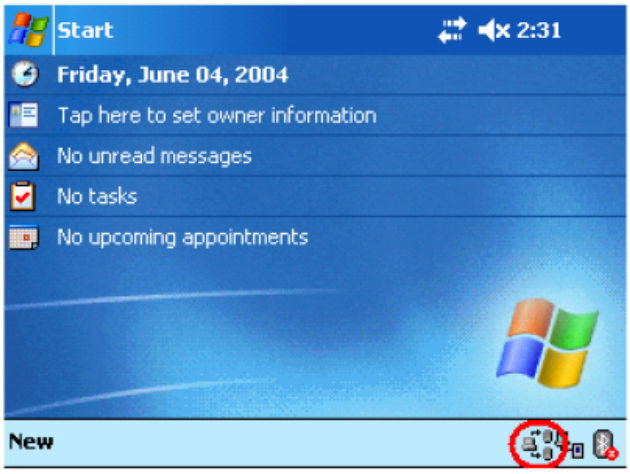


Figura 6: servidor de FTP identifica-se através de ícone na área de trabalho

Para isso, primeiramente localizamos o trecho de código responsável pela exibição do ícone na barra de tarefas. Graças ao recurso de listagem de nomes de função do "*IDA Pro*", detectamos uma delas chamada "*Shell_NotifyIcon*". Depois de encontrada, o seu código foi alterado da seguinte forma:

```
MOV Shell_NotifyIcon    para        MOV R0,
R03A 01 00 EB           para        00 00 A0 E1
```

O lado esquerdo mostra o comando original, seguido dos valores em hexadecimal originais. Para impedir a exibição do ícone, o código foi alterado para que o programa não realizasse nenhuma operação (Na verdade foi alterado para realizar um NOP virtual, fazendo com que o conteúdo de R0 fosse copiado para o próprio R0).

A porta padrão também foi alterada de 21 para uma de valor mais alto, que provavelmente não chamaria muito a atenção. Esta alteração é tão fácil quando localizar o valor absoluto da porta em questão e alterá-lo para o de preferência.

2.1.13. Controle remoto

Para o próximo exemplo, encontramos uma aplicação que nos permite acessar remotamente um dispositivo executando Windows Mobile: *vRemote*. Neste caso, o programa exibie uma janela sempre que é iniciado, o que alerta o usuário de sua presença, o que queremos retirar.

Figura 7: Janela exibida ao iniciar a aplicação VirtualCE

A seguir mostramos as alterações feitas na aplicação para remover completamente qualquer sinal visual indicador da presença do *vRemote* sendo executado.

```
BL ShowWindow     para  MOV R0, R0 (Virtual NOP)
A6 15 00 EB       para  00 00 A0 E1
```

Novamente, fomos capazes de fazer tais alterações fazendo uso do "*IDA Pro*" e tendo como alvo a função "*ShowWindow*", sobreescrevendo-a com um trecho de código com NOP e mais duas outras partes que faziam referencia a esta função.

A questão destes exemplos é que aplicações comuns para Windows Mobile podem ser facilmente modificadas. Mais informações sobre alteração de aplicação em baixo nível podem ser encontradas no livro "*Aggressive Network Self Defense*". O primeiro capítulo do livro entra em

detalhes sobre como duas pessoas, cada uma portando seu Pocket Pc, podem travar uma batalha digital através de modificações de código em baixo nível.

2.2. Descrição de ameaças específicas

O Windows Mobile ainda não atraiu muita atenção no que diz respeito à versões publicamente conhecidas de vírus e cavalos de tróia. Até Agosto de 2005, somente duas aplicações maliciosas criadas para Windows Mobile foram identificadas. Apesar deste número ser pequeno, a sofisticação tecnológica empregada é grande, como descrito a seguir.

3. Ataques através da Rede

A plataforma Windows Mobile foi desenvolvida para dispositivos operados em redes sem-fio. E também é vulnerável a muitas das ameaças que existem para o mundo dos PCs. A seguir, descrevemos uma série de ataques que podem ser feitos contra um PDA localizado em uma rede sem-fio sem que haja prévia manipulação direta do dispositivo.

3.1. Classificação geral de tipos de ataques

3.1.1. Formas de ataques genéricas

Os PDAs geralmente usam um adaptador de rede sem fio com baixo consumo de energia. A partir de então, pode-se acessar a Web, e-mails, etc. Considerando que o equipamento trabalha com baixas taxas de consumo de energia, a intensidade do sinal *wireless* utilizado também é baixa. Sendo assim, é relativamente fácil provocar um nível de interferência (utilizando um "*Acess Point*" ou até mesmo um laptop) suficiente para impedir que o dispositivo possa se conectar ao local correto, mas induzindo-o a se conectar em um ponto de acesso "mal-intensionado" (*rogue access point*).

Além disso, algumas vezes é possível realizar um ataque de negação de serviço do tipo "*ping DoS*", que irá consumir todos os recursos disponíveis do PDA, fazendo com que fique extremamente lento, impraticável de se trabalhar.

Por final, pode-se também atacar serviços em PCs, por exemplo o *Active Sync** na porta 901, o que irá impedir que um PDA associado possa se conectar.

3.1.2. Quebra de chave da criptografia

Atualmente, diversas tecnologias de criptografia são empregadas para proteção dos dados trafegados nas redes sem fio. No início, na maioria dos casos nenhuma criptografia era utilizada, sendo possível para qualquer pessoa nas proximidades da rede observar o tráfego em texto puro (incluindo credenciais de usuários, mensagens de correio eletrônico, etc). A questão evoluiu para um sistema de criptografia fraco, chamado WEP (Wired Equivalent Privacy), burlada pouco tempo depois de seu lançamento, devido à sua chave ser estática e de tamanho reduzido.

Atualmente, os sistemas de autenticação já adquiriram uma maturidade aceitável, fazendo uso de certificados digitais como método de autenticação e chaves de criptografia dinâmicas. Os ataques de quebra de chave de criptografia pretendem burlar tais sistema, de modo a capturar o tráfego de forma não criptografada.

3.1.3. Tomada de controle do dispositivo

A literal invasão de dispositivos móveis significa a tomada de controle do equipamento, de forma a utilizá-lo remotamente como se fosse de forma local. Diferentes níveis de acesso podem ser obtidos, de acordo com a porta de entrada utilizada. Esta última pode ser uma porta dos fundos instalada através de um cavalo de tróia ou até mesmo através da exploração de uma vulnerabilidade crítica em alguma aplicação. Pode-se dizer que este tipo de ataque é o mais perigoso, pois pode oferecer controle completo do sistema.

3.1.4. Pontos de acesso falsos

Uma das formas mais práticas para se obter credenciais de usuários, é induzí-los a tentaram efetuar uma conexão sem fio e se autenticar em um ponto de acesso falso (chamados na literatura de *rogue access points*). O usuário descuidado irá identificar um ponto de acesso com o mesmo nome da rede que está acostumado a usar e rapidamente tem as suas credenciais capturadas. Existem ferramentas que emitem *beacons* (pacotes transmitidos para notificar os usuários da presença de uma rede sem fio) simulando a existência de diversas redes, confundindo usuários e até mesmo wardrivers (atacantes que circundam áreas buscando redes sem fio de interesse). Este tipo de ataque se aplica às tecnologias 802.11 e Bluetooth, mas principalmente à 802.11.

3.1.5. Visão geral de worms/virus conhecidos

A partir do final de 2005, virii disseminàveis por redes sem fio cresceram num ritmo grande em número e sofisticação. Como exemplo, o primeiro vírus para Pocket PC (Dust) a aparecer era incrivelmente complexo. Tinha uma tecnologia de penetração equivalente ao vírus Chernobyl Win32, que foi o primeiro vírus para PCs a quebrar o Anel 0, protegido pelo sistema operacional Windows.

Além disso, menos de um ano depois do Dust, inúmeras ameaças foram identificadas. Por exemplo, criadores de vírus têm desenvolvido trojans e têm os combinado com a capacidade de propagação do vírus Carib (Cabir) via Bluetooth. Em um ano, houve uma evolução de vírus equivalente aos 20 anos que levou para PCs.

O problema devido à rápida evolução de ameaças é o fato de que os dispositivos móveis atuais não suportam softwares de antivírus sofisticados nas plataformas correntes. Por exemplo, sistemas operacionais embutidos não usam interrupções (chamadas de sistema para o kernel), então uma heurística de vírus no PDA ou Smartphone não pode bloquear uma interrupção específica caso haja suspeita de vírus.

Outro problema é a aparência enganosa e obsoleta da indústria de antivírus. A velha proteção desta, freqüentemente opera através de um princípio antiquado de “segurança através da incerteza”.

O Trojan Brador

O Brador foi o primeiro trojan para Pocket PC. Ele dá total controle remoto do dispositivo a um hacker que pode estar até do outro lado do mundo. Isso é um problema principalmentepara executivos ou administradores de rede que, como muitos outros, usam o Pocket PC para controlar toda a infraestrutura da empresa.

O Brador é um sucesso em parte, pois o sistema operacional do Pocket PC não vem com um monitor de processos nativo. Sem um monitor de processos, é difícil identificar e remover trojans. No Pocket PC falta esse recurso e quando um usuário tenta apagar o arquivo malicioso, o sistema apresenta uma mensagem de erro dizendo que o programa está em uso. Neste caso, o único jeito de remover o trojan seria realizando o reset de fábrica do sistema. Felizmente, existem ferramentas apropriadas que fazem isso sem a necessidade da restauração completa.

3.2. Ataques via interface Bluetooth

Ataques via *bluetooth* tem sido destaque já há algum tempo. No entanto, quando se chega mais perto para analisá-los, percebe-se que em sua grande maioria os alvos são telefones celulares, não PDAs. Apesar disso, existem alguns problemas que devem ser endereçados. É importante ressaltar que estes problemas podem ou não estar presentes no seu equipamento, dependendo da implementação da tecnologia empregada pelo fabricante do mesmo.

O primeiro ataque é chamado "*bluejacking*", o que não é nada além do envio de mensagens para um dispositivo móvel com a interface *bluetooth* habilitada. O próximo problema que pode afetar usuários de PDA´s são os ataques de negação de serviço via *bluetooth*. Uma das formas de fazê-lo é enviando um pacote do tipo *ping* para o dispositivo, que poderá alocar os recursos, fazendo com que ninguém mais possa se conectar. Existem outros ataques que podem desabilitar ou tirar serviços de operação.

"*PIN cracking*" é a última forma de ataque que mencionamos. Como o *BlueTooth* é protegido por uma senha de apenas 4 dígitos (*PIN - personal identification number*), torna-se fácil realizar um ataque de força bruta e descobrí-la. Normalmente isso pode ser conseguido em algumas horas, dependendo de quantos clientes estão atacando o alvo. É possível também encontrar dispositivos ocultos através de força bruta aplicada a endereços físicos (*MAC addresses*) de interfaces de rede *bluetooth*.

3.2.1. Varrendo endereços Bluetooth

O endereço MAC Bluetooth é uma seqüência de 6 bytes que identifica o dispositivo. Os primeiros 3 bytes são atribuídos pelo IEEE e identificam o fabricante do equipamento. Os últimos 3 bytes são atribuídos pelo próprio fabricante.

Em teoria, habilitar o modo invisível deveria proteger os usuários de conexões não autorizadas. Na prática, mesmo assim ainda é possível localizar tais dispositivos. Existem ferramentas, por exemplo, que realizam ataques de força bruta em busca de dispositivos invisíveis. Uma dessas ferramentas é o "RedFang"[31], criada por Ollie Whitehouse [9], que tenta se conectar a todos os endereços físicos possíveis, até que receba respostas para tais tentativas de conexão. Na verdade, esta ferramenta é mais uma prova de conceito do que de fato uma ferramenta de hacking. O principal obstáculo na verdade é o tempo necessário para se realizar o ataque, pois a verificação de apenas um dispositivo leva de 2.5 a 10 segundos em média.

Para se ter uma noção melhor, temos que o espaço de endereçamento da Sony Ericsson [10] comporta 16.777.216 possíveis endereços. Se assumirmos que a verificação de cada dispositivo leva 6 segundos, a varredura total levará 1165 dias, o que significa que levaria três anos para encontrar todos os dispositivos da Sony Ericsson [10] escondidos em uma sala. Percebe-

se, assim, que não esta é uma forma efetiva de se obter tais informações. Exatamente por isso foram criadas novas técnicas, que realizam o mesmo serviço de forma muito mais eficiente.

3.2.2. Reduzindo a margem de endereços possíveis

Em primeiro lugar, caso o fabricante seja conhecido, o número de endereços possíves é imediatamente limitado a 16.777.216 alternativas. Além disso, alguns dispositivos Bluetooth costumam utilizar faixas de endereços mais previsíveis, de acordo com o modelo. Por exemplo, o endereço da maioria dos celulares Sony Ericsson P900 [10] começa com os seguintes sete dígitos hexa "00:0A:D9:E", o que significa que restam somente cinco dígitos hexadecimal para serem descobertos. Esta informação reduz a busca de mais de 16 milhões de endereços para apenas 1.048.576 possibilidades! Além disso, o quarto byte do endereço costuma estar na faixa "E7-EE", o que reduz ainda mais o número de possibilidades para 524.288. Com isso, o ataque de força bruta levaria 36 dias, que apesar de já ser absurdamente menor, mesmo assim não é prático.

O tempo necessário para realizar a varredura não só pode ser diminuído pela redução das faixas de endereçamento, mas também pela aceleração do processo de varredura. A versão atual do "RedFang" [31] permite a distribuição do trabalho da varredura entre diferentes dispositivos. Se usarmos oito dispositivos para isso, reduzimos o tempo total da busca por celulares Sony Ericsson [10] para quatro dias e meio. Apesar deste tempo ser relativamente alto, pode-se esperar a redução deste tempo através de técnicas mais avançadas.

3.2.3. Descobrindo endereços Bluetooth enquanto se comunicam

Endereços MAC Bluetooth podem ser descobertos observando o tráfego de comunicação entre dispositivos, pois o endereço em si não é criptografado mesmo que o usuário utilize criptografia.

Este é um dos principais problemas com a especificação do Bluetooth. O chaveamento de freqüência em uso pelos dispositivos que ocorre 1600 vezes por segundo fornece uma proteção básica ao tráfego não criptografado. No entanto, o chaveamento de freqüências ocorre de forma pseudo-randômica, o que significa que um hacker com as ferramentas necessárias poderia sincronizar com um padrão pré-definido de chaveamento entre dois dispositivos em comunicação. Além disso, a seqüência usada no chaveamento é compartilhada para todos os membros da mesma piconet (rede de dispositivos BlueTooth), o que dá boa vantagem ao hacker. Na verdade, já existem equipamentos no mercado que são capazes de capturar tráfego Bluetooth com grande facilidade e analisá-lo, mas ainda custa muito caro (em torno de U$ 10.000), o que dificulta a aquisição para a maioria dos hackers.

Os hackers podem tirar proveito de pessoas descuidadas que deixam seus telefones no modo visível. Às vezes, é necessário deixá-los temporariamente no modo visível para fazer o

primeiro contato com um novo dispositivo - pairing, descrito mais a frente. Esta necessidade de tornar o dispositivo visível é uma grande vantagem para os hackers, pois podem se aproveitar deste curto espaço de tempo quando os dispositivos se tornam visíveis e até mesmo de esquecimentos de revertê-los para o modo invisível. Quando visível, os hackers podem descobrir o endereço do dispositivo instantaneamente. Nenhum dos celulares com Bluetooth do mercado permitem a entrada manual de um endereço para a realização de sincronização com outro dispositivo (pairing), o que significa que obrigatoriamente o celular deve ficar em modo visível para ser encontrado e realizar a comunicação. Como o endereço do dispositivo é único e imutável, basta o atacante descobrí-lo somente uma vez. Ou seja, basta que o dispositivo fique visível por um curto espaço de tempo para o hacker descobrir seu endereço, e mesmo que retorne ao modo invisível, o atacante poderá se conectar, sem que seu dono possa negar esta conexão. Isso acontece, pois um dispositivo Bluetooth nunca nega uma conexão básica L2CAP. Os dispositivos atuais não bloqueam esse tipo de conexão por se tratar de uma conexão de baixo nível, não existe ainda esta funcionalidade, nem mesmo bloqueio por endereços. Por padrão, não existe um firewall para Bluetooth.

3.2.4. Comunicação via Bluetooth entre dispositivos & segurança

Umas das principais funções que envolve segurança de Bluetooth é a comunicação entre dois dispositivos (pairing). Por padrão, a comunicação não é autenticada, e praticamente qualquer dispositivo pode se conectar a qualquer outro. No entanto, para acessar determinadas funções como transferências de arquivos, normalmente exigi-se uma autenticação, baseada em uma chave simétrica, cadastrada em ambos os dispositivos (PIN codes ou passkeys).

Figura 8: Exemplo de configuração da autenticação de uma configuração Bluetooth.

Uma vez esta chave cadastrada, é gerada uma chave de sessão, que é armazenada na memória e possibilitará a comunicação entre estes mesmos dispositivos no futuro sem passar por esta fase de autenticação novamente.

3.2.5. Problemas relacionados a fabricantes

Infelizmente para os usuários de dispositivos Bluetooth, o processo de autenticação e autorização para acessar serviços não é corretamente implementado pelos desenvolvedores. Estas fraquezas já afetam alguns aparelhos e permitem o roubo de agendas de telefone, informações de calendário, fotos e até mesmo a efetuação de ligações telefônicas ou envio de SMS a partir do dispositivo atacado. Tudo devido à falta de controle de acesso adequada.

Apenas para ilustrar o perigo potencial, imagine que alguém tomou o controle do telefone celular de um indivíduo e envia uma mensagem de SMS para a polícia com uma ameaça. Automaticamente a polícia irá identificar o nome a que está associado à linha telefônica de origem, chegando facilmente ao dono do aparelho invadido. O indivíduo culpado terá ainda bastante dificuldade de provar que nada fez, pois normalmente não há registro das conexões via Bluetooth.

A vulnerabilidade de segurança mencionada é facilmente explorada e não requer nenhuma habilidade especial. Apenas dois comandos comuns são necessários para roubar uma agenda telefônica de um aparelho T610:

```
# hcitool scan
Scanning .

00:0A:D9:15:0B:1C T610-phone

# obexftp -b 00:0A:D9:15:0B:1C --channel 10 -g telecom/pb.vcf -v
Browsing 00:0A:D9:15:0B:1C ...
Channel: 7
No custom transport
Connecting...bt: 1
done
Receiving telecom/pb.vcf...\done
Disconnecting...done
```

Isso é tudo o que se faz necessário para roubar informações de um aparelho T610 inseguro. Ambos os commandos "hcitool" e "obexftp" são comandos típicos de Bluetooth, disponíveis em qualquer distribuição Linux [12] com o pacote de expansão Bluetooh.

Esta vulnerabilidade foi descoberta por Adam Laurie [26] e afeta diversos dispositivos, incluindo: Nokia [27] 6310, 6310i, 8910, 8910i, Sony Ericsson [10] T68, T68i, R520m, T610, Z600 e possivelmente outros. Foi profundamente estudada pelo grupo "trifinite", que inclusive desenvolveu uma aplicação chamada "Blooover", que explora a vulnerabilidade.

Não é uma surpresa que alguns usuários menos experientes destes dispositivos, por exemplo, aqueles que só precisam fazer ligações ou enviar mensagens de testo, tenham conhecimento de que seus aparelhos celulares precisam receber atualizações de software. É mais incrível ainda observar que dispositivos com falhas tão sérias podem estar ainda no mercado. Qualquer auditoria de segurança na fase de testes do sistema operacional (antes de disponibilizar no mercado) deveria apresentar tais resultados. Ou seja, fica claro que alguns fabricantes destes dispositivos não se importam muito com a segurança, o que traz uma espectativa de que o número de falhas de segurança cresça ainda mais no futuro.

3.2.6. O Risco de conexão à APs falsos

O procedimento de sincronização de dispositivos apresenta mais um risco. A lista de dispositivos descobertos apresenta somente seu nome, e não seu endereço Bluetooth.

Figura 9: A descoberta de dispositivos não divulga seu endereço Bluetooth

Como o dispositivo tem um nome, ele pode ser facilmente modificado pelos usuários. Portanto, não deveria ser usado como um identificador único do dispositivo no processo de sincronização; O endereço Bluetooth realmente deveria ser comparado para verificações complementares.

Este pequeno detalhe poderia ser explorado de diversas maneiras, especialmente em serviços oferecidos publicamente através de Bluetooth. Por exemplo, um Ponto de Acesso (Access Point – AP) poderia ser substituído por outro com fins maliciosos, porém com o mesmo nome e aceitando as mesmas informações de autenticação dos usuários. No entanto, todas as informações que passarem por ele serão capturadas e analisadas, em busca de senhas e informações sigilosas.

Este ataque também pode ser executado de forma alternativa. Em muitos lugares públicos, existem quiosques destinados à propaganda de produtos, e muitas vezes oferecendo conteúdo via Bluetooth, como, por exemplo, toques para celular e jogos.

No caso, quando o usuário selecionou o conteúdo a ser copiado, automaticamente o nome do dispositivo do transmissor deste conteúdo é inserido na lista de contatos. O problema é que o dispositivo que se intitula “MOBILE-KIOSK", não necessariamente é quem diz ser. Tal “visitante” poderia ser um hacker que alterou o nome de seu notebook para “MOBILE-KIOSK". Certamente, estes ataques poderiam ser evitados caso o processo de autenticação fosse melhor implementado, pois atualmente são implementados de forma pobre e as senhas normalmente são estáticas (ou seja, não existe uma política de alteração de senhas periodicamente).

3.2.7. Ataques específicos

Bluejacking - Consiste no envio de mensagens, inclusive spam, para dispositivos eletrônicos alheios via bluetooth. A técnica surgiu inocentemente, quando um usuário identificou nas proximidades um telemóvel Nokia [27] com Bluetooth ativo e enviou, por diversão, uma mensagem que dizia "Compre Ericsson". Empresas de marketing levaram o conceito adiante e criaram o *Bluecasting*, em que um equipamento especial dispara propaganda para todos os aparelhos que passam perto. A prática é classificada como spam e proibida em muitos países.

Bluesnarfing – Consiste em roubo das informações dos aparelhos alheios. Basta que o dispositivo (só os modelos mais antigos são vulneráveis) esteja com o Bluetooth ativado e em modo visível para que uma pessoa mal-intencionada nas proximidades possa invadí-lo e roubar o conteúdo da agenda e catálogo de endereços, por exemplo.

Bluetooth Sniping - Embora o alcance típico de um dispositivo Bluetooth seja de 10m e de um laptop possa chegar a 100m, um grupo de pesquisa em aplicações sem fio, construiu um "rifle bluetooth" capaz de captar sinais de dispositivos localizados a mais de 1 km. Apesar da aparência ameaçadora, o equipamento é apenas um transmissor/receptor de alta potência acoplado a uma antena direcional que deve ser apontada para o alvo. Um micro portátil recebe os sinais da antena e mostra as identificações dos aparelhos bluetooth, abrindo caminho para ações de Bluejacking e Bluesnarfing. Durante os testes do equipamento em Los Angeles, o grupo conseguiu encontrar dezenas de aparelhos Bluetooth em minutos, simplesmente apontando a "arma" para prédios comerciais ao redor. A brincadeira recebeu o nome de Bluetooth Sniping.

Ataques de SMS - Uma vulnerabilidade em potencial do SMS é permitir que um dispositivo receba ou envie uma mensagem a qualquer momento, independente se uma ligação de voz ou dado esteja em andamento. Se o dispositivo estiver indisponível, a mensagem será armazenada no servidor central. O servidor, então, irá tentar retransmitir a mensagem até que possa entregar a mensagem.

De fato, há ferramentas que são usadas para inundar serviços de SMS. O mesmo princípio destas, quando unido com o poder de replicação de um vírus, pode potencialmente resultar em ataques de Negação de Serviço em ampla escala. Outro exemplo de uma inundação de vírus de SMS que ocorreu na Escandinávia. Quando um usuário recebia uma mensagem, o vírus bloqueava os botões do dispositivo, o que se tornou um ataque de Negação de Serviço contra todo o sistema. De maneira semelhante, uma empresa norueguesa encontrou um outro exemplo de código malicioso. Eles encontraram um certo SMS que congelava telefones que recebiam esta mensagem. O código impedia o uso do teclado logo que o SMS era recebido.

Carib (Caribe, Cabir)

Primeiro vírus conhecido para Bluetooth, alvo de telefones móveis. Mesmo o próprio vírus sendo relativamente inofensivo, ele representa uma nova era para criadores de vírus e um novo conjunto de preocupações para os proprietários de telefones móveis.

Um vírus pode ser escrito, infectar um único dispositivo e provavelmente terá vida curta. Para manter o vírus vivo, ele deve ser capaz de se propagar de um dispositivo para outro. Isso é chamado de "infector" ou vetor de infeccção. Enquanto vetores de infecção têm mudado e evoluído ao longo dos anos, o mais comum é via e-mail. Uma vez um dispositivo infectado, o vírus usa seu próprio mecanismo de envio de e-mails ou o cliente de e-mail da vítima para se disseminar para os e-mails que encontra no sistema. Outros vetores de infecção são drives de disquete e software pirata. Novos vetores são raros simplesmente porque há um número limitado de novos métodos de comunicação.

Apesar do conceito de descobrimento de dispositivos via Bluetooth ser excelente, nos últimos anos diversas vulnerabilidades têm sido encontradas no protocolo que torna possível a obtenção de informações de usuários, envio de mensagens não solicitadas e realização de outros ataques. Entretanto, até agora esses "ataques" têm sido feitos somente em laboratório ou para mandar mensagens não solicitadas a outros dispositivos Bluetooth.

Embora o worm Caribe em si seja inofensivo, recentemente tem sido misturado a outros malwares, criando novas ameaças. Uma vez o dispositivo infectado, ele varre outros dispositivos Bluetooth até encontrar um (e somente um). Depois, tenta enviar para o alvo uma cópia de si. Neste ponto, a vítima é instigada com uma caixa de diálogo, que pergunta se a pessoa gostaria de aceitar o arquivo que chega. Se a vítima aceitar, o arquivo se transferirá e outro prompt aparecerá alertando que a origem do arquivo não pôde ser verificada. Se a vítima escolher a opção "Continuar", o dispositivo irá perguntar à vítima pela última vez se deseja mesmo instalar o programa. Neste ponto, o dispositivo já está infectado.

Uma vez infectado, uma tela aparece no dispositivo da vítima com a mensagem "Caribe-VZ/29a". Então, o dispositivo infectado começa a varrer outros que possam ser infectados.

O Caribe transferirá o arquivo uma única vez. Além do mais, somente telefones Nokia [27] da série 60 mostram-se vulneráveis, pelo menos de acordo com um memorando interno escrito pela Symbian. Ainda, esse worm requer interação de um usuário sem conhecimento algum, pois três alertas são emitidos, dificultando a disseminação do Caribe. Quer dizer, até que ele seja misturado a outro malware. Apesar deste worm não se aplicar ao escopo de sistemas operacionais deste trabalho, é interessante citar o caso do Caribe por ser o pioneiro a se espalhar via Bluetooth.

3.3. Ataques via interface IEEE 802.11

Ataques a PDAs em redes sem fio não são um problema específico dos PDAs. No entato, considerando que a maioria dos usuários de PDAs possuem uma conexão Wi-Fi para ler/responder e-mails, conectar-se ao escritório ou acessar a Internet, devemos considerar este vetor de ataque.

Resumidamente, podemos dizer que o usuário do PDA poderá ser atacado das seguintes formas: quebra da chave criptográfica WEP (*Wired Equivalent Privacy*), quebra da chave criptográfica WPA (*Wi-Fi Protected Access*), ataques "*Man in The Middle*" (MiTM), injeção de conteúdo Web, ataques passivos (coleta de tráfego), pontos de acesso maliciosos (rogue *acess points*), ataques de negação de serviço e estouro de pilha (buffer overflow).

Através destes, um atacante pode interceptar mensagens de correio eletrônico, obter acesso à rede interna de empresas, capturar senhas, enganar usuários induzindo-os a acessar páginas com código malicioso, dentre outros.

3.3.1. Ataques ao WEP

Diversas falhas no algoritmo WEP foram encontradas, que seriamente colocam em dúvida a sua confiabilidade. Em particular, as ameaças mais conhecidas são:

- Ataques passivos para decriptar tráfego baseado em análise estatística.
- Ataques ativos para injeção de tráfego a partir de estações não autorizadas.
- Ataques ativos para decriptar tráfego, baseados na manipulação de pontos de acesso.
- Ataques baseados na criação de dicionários construídos a partir de tráfego coletado, que permite a decriptação automática de tráfego em tempo real.

Todos os ataques citados podem ser realizados com equipamentos de baixo custo e de fácil aquisição. Além disso, se aplicam tanto ao WEP de 40 quanto ao de 128 bits e ao padrão 802.11b, uma extensão para suportar maiores taxas de transmissão, mas que manteve intocada a implementação do WEP. Vamos apresentar com mais detalhes somente o primeiro tipo de ataque, por ser o mais comum.

Ataque passivo para decriptação de tráfego

Este ataque é possível devido ao seguinte fato: uma pessoa pode capturar todo o tráfego encriptado da rede sem fio até que uma colisão do vetor IV seja identificada. Ao aplicar a função lógica XOR entre dois pacotes que usam este mesmo vetor de inicialização (IV), o atacante automaticamente obtém o resultado do XOR do texto puro das mensagens de cada pacote. O resultado obtido pode ser usado para se fazer inferências sobre o conteúdo destas. Como o tráfego IP é bastante previsível e inclui diversas redundâncias, estas podem ser usadas para dar várias dicas sobre o conteúdo das mensagens. Tentativas de adivinhação mais inteligentes são usadas posteriormente e algumas vezes conseguem identificar todo o conteúdo da mensagem.

No entanto, quando tais "adivinhações estatísticas" baseadas em apenas dois pacotes não são insuficientes para identificar o conteúdo da mensagem, é possível trabalhar com outros pacotes cujo vetor IV também colidiu. Em um tempo relativamente pequeno, é possível cotetar tráfego encriptado com a mesma chave, fazendo com que a qualidade da análise estatística cresça rapidamente. Uma vez que seja possível desencriptar toda a mensagem, todos os outros pacotes que usam o mesmo vetor IV poderão ser desencriptados automaticamente.

3.3.2. Ataques ao WPA

Atualmente, a única forma de atacar o algoritmo WPA é causando uma re-autenticação forçada de um usuário que esteja utilizando a rede. É necessária uma conexão real e pode ser necessário esperar para que a re-autenticação aconteça.

Ataque de re-autentiucação forçada

Neste ataque simples e efetivo, basta forçar um usuário ativo a se re-autenticar e capturar o tráfego da re-conexão e re-autenticação, o que economiza tempo, pois não é mais necessário esperar até que ocorra uma re-autenticação espontânea. Após alguns segundos, a re-autenticação já deve estar completa e poderá ser feito um ataque de dicionário contra a chave primária de encriptação – PMK (primary master key).

3.3.3. Ataques de invasão de memória (Buffler Overflow attacks)

O Windows Mobile é tão vulnerável a ataques de invasão de memória (ou estouro de pilha em algumas traduções) quanto a sua família de grandes irmãos. O próprio servidor de FTP usado para os testes é dotado de um. O executável "ftpsvr.exe" implementa comandos comuns de FTP, mas infelizmente não verifica os parâmetros passados. Isso significa que um atacante pode sobrescrever a pilha de execução com código assembly e ter este código arbitrário executado.

Mesmo que alguns detalhes possam variar entre dispositivos e versões de sistema, vamos mostrar que é possível fazer um ataque via rede e injetar código que irá causar um "*hard reset*" no PDA. Felizmente, esse tipo de ataque é relativamente limitado em PDAs. Como não existe efetivamente uma shell de comando, um ataque para ser completo requer um *upload* de alguma aplicação para que o controle total do sistema seja obtido. Já citamos um exemplo de aplicação como esta anteriormente: o calavo de tróia "brador.exe".

3.3.4. Captura de tráfego

Um *sniffer* provê a seu utilizador uma visão do tráfego passante na rede. Atualmente, a maioria das redes cabeadas é baseada em switchs, o que dificulta muito este tipo de ataque (mas não o torna impossível). Neste caso, estamos falando de redes onde os PDAs normalmente não estão conectados. No caso de uma rede sem fio, esta funciona de forma parecida com um HUB (topologia em barra), pois todos "escutam" o tráfego da rede (claro, desde que estejam presentes na localidade de sinal). Como a entrada e saída de Pockets PCs, Smartphones e derivados nas mãos ou bolsas de visitantes em empresas não são muito controladas, torna-se fácil capturar tráfego wireless para futura análise.

Alguns *sniffers* para Windows Mobile necessitam que o dispositivo esteja conectado a alguma rede antes que possa capturar tráfego. No entanto, esta dificuldade não existe nos *sniffers* para Linux, podendo facilmente capturar o tráfego do canal desejado (*Kismet* e *tcpdump* são exemplos de tais ferramentas). A figura a seguir mostra a captura de tráfego de um usuário da rede quando acessava a página do Google, utilizando o *vxSniffer*:

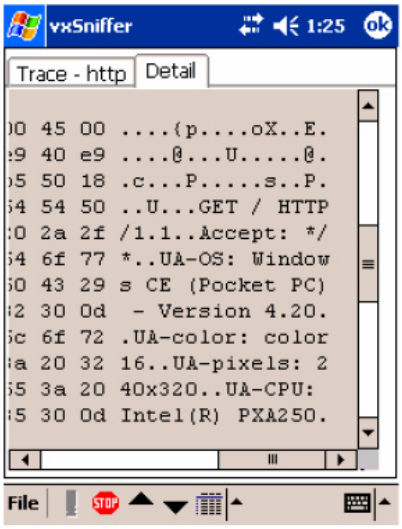


Figura 10: vxSniffer em ação

É importante ressaltar que um Pocket PC, por exemplo, suporta interface Ethernet, além da wireless, o que permite a sua conexão direta a um *HUB* ou *switch* e mais uma vez, capturar tráfego.

3.3.5. Análise de vulnerabilidades

Uma vez dentro da rede, os PDAs podem realizar o mesmo tipo de varredura que um PC. Varreduras através de requisições ICMP, por serviços conhecidos e até mesmo exploits podem ser executados a partir de um equipamento como este. Por exemplo, um iPAQ rodando Linux [12] pode ser usado para executar a ferramenta mais conhecida de varradura de redes, *Nmap*. O Linux [12] pode ir além, pois facilita muito a criação de scripts em *Perl*, que podem ser usados para diversos tipos de teste de invasão.

3.3.6. Abrindo portas para um ataque

A seguir, discutiremos sobre um método simples de se obter acesso anônimo e remoto a uma rede wireless, transformando o PDA em uma verdadeira porta dos fundos feita em *hardwar*. O propósito disso é apenas mostrar o quanto se pode ir longe ao se atacar redes wireless usando PDAs para que a conciência da necessidade de se aumentar o nível de segurança nas corporações seja levada à sério.

1. Instalar uma distribuição do Linux [12] de acordo com a preferência
2. Instalar drivers necessários para o funcionamento das interfaces wireless e Ethernet
3. Criar um script de configuração da interface wireless para inicar em modo *ad-hoc* após a inicialização do sistema. O uso de criptografia é opcional. A interface deve começar a operar em algum canal livre, à escolha.
4. Instalar as aplicações SSH, Nmap e tcpdump no PDA.
5. Vá até o local desejado e conecte a interface *ethernet* à rede, de forma que fique bem escondido.
6. Ligue o PDA.
7. A partir de um *laptop* ou outro PDA, conecte-se ao equipamento via IP pré-estabelecido, usando túnel SSH.
8. Agora, pode-se usar o *tcpdump* para capturar tráfego da rede, identificando endereçamento para então alterar o correspondente na interface Ethernet

4. Checklist de Segurança para dispositivos móveis em redes sem-fio

A seguinte tabela fornece uma checklist de segurança para PDAs e Smartphones. Esta apresenta boas práticas de uso e recomendações para se criar e manter um ambiente seguro para o uso destes dispositivos. A primeira coluna (Boa Prática), caso marcada, significa que a informação deve ser implementada. A segunda (Deve-se considerar), significa que a recomendação deve ser fortemente analisada por três motivos:
primeiro, irá aumentar o nível de segurança do ambiente através do oferecimento de um tipo de proteção complementar, segundo, a recomendação utiliza a técnica de segurança em camadas (defense-in-depth strategy). Terceiro, trará impactos de performance, operacionais e custo. Em resumo, cada organização deve avaliar o custo benefício da implementação.

Recomendação de segurança		Checklist	
		Boa prática	Deve-se considerar
1	Desenvolver uma política de segurança para a organização, que direcione o uso de todos os dispositivos de computação móvel.	√	
2	Assegurar que os usuários da rede são treinados (security awareness) quanto aos riscos de segurança e estão cientes dos inerentes a dispositivos de computação móvel.	√	
3	Realizar uma avaliação de risco para entender o valor dos bens presentes na organização que necessitam de proteção.	√	
4	Conduzir práticas de auditoria esporádicas, mas continuamente, para monitorar e possivelmente detectar incidentes de segurança ligados à dispositivos de computação móvel.	√	
5	Assegurar que os limites de acesso físico por vias externas às dependências da organização são suficientes em termos de proteção, para todo o perímetro de prédios da organização.	√	
6	Fazer uso de controles de acesso físico nos prédios e outras áreas (Como identificação por crachás com fotografias, cartões inteligentes, biometria e outros).	√	
7	Minimizar o risco de perda ou roubo através do uso de fechaduras e cabos de segurança.		√
8	Identificar todos os dispositivos móveis com o nome do proprietário e informações de contato da organização.	√	

9	Assegurar que os usuários saibam onde reportar a perda ou roubo do um dispositivo.	√	
10	Assegurar que os dispositivos são guardados de forma segura quando fora de uso.	√	
11	Certifica-se de que módulos adicionais (periféricos, cartões de memória, etc) estão protegidos adequadamente quando fora de uso, como prevenção contra roubos.	√	
12	Habilitar o pedido de senha ao se ligar cade dispositivo de computação móvel.	√	
13	Criar e manter uma política de manutenção de senhas adequada, (troca de senhas periodicamente, normas de formação, etc).	√	
14	Assegurar que aplicativos de sincronização com dispositivos móveis instalados nas estações de trabalho são protegidos por senha.	√	
15	Armazenar dados necessários em módulos apropriados e de forma encriptada.		√
16	Visitar freqüentemente websites de fabricantes em busca de correções e versões mais recentes dos softwares utilizados.	√	
17	Instalar correções de software em dispositivos e estações de trabalho afetadas.	√	
18	Review security-related mailing lists for the latest security information and alerts. Acompanhar listas de discussão relacionadas na Internet para obter as últimas informações e alertas de segurança.	√	
19	Assegurar que todos os dispositivos tenham mecanismos de bloqueio automático após um período de inatividade.	√	
20	Sincronizar regularmente dispositivos com suas respectivas estações de trabalho.	√	
21	Evitar armazenar informações confidenciais no dispositivo móvel. Se necessário, deve-se movê-las para um local mais seguro quando possível.	√	
22	Desligar em períodos de inatividade, portas de comunicação do dispositivo.	√	
23	Instalar software de antivírus em todos os dispositivos móveis.	√	

24	Instalar firewalls pessoais em todos os dispositivos móveis.		√
25	Assegurar que os PDAs são disponibilizados para os usuários com software/firmware de controle de acesso.		√
26	Instalar clientes de VPNs em todos os dispositivos móveis que transmitem dados através de redes wireless.		√
27	Assegurar que um usuário possa ser autenticado de forma segura local ou remotamente, para acessar os recursos da organização.	√	
28	Usar criptografia robusta e utilitários de proteção de senha para proteger dados sensíveis e aplicações.	√	
29	Usar soluções de segurança adequada ao tamanho da organização para gerenciar a segurança de dispositivos de forma centralizada.		√
30	Assegurar que ferramentas de análise de segurança são usadas para avaliar dispositivos móveis.		√
31	Quando dispositivos não forem mais ser utilizados, todas as configurações e dados devem ser apagados adequadamente, evitando a possível exposição de informações sensíveis.	√	

5. Avaliação Prática

5.1. Testes com Emuladores vs Teste com dispositivos físicos

5.1.1. Descrição do ambiente de testes com emuladores

Além do trabalho teórico, foram realizados testes básicos usando emuladores dos seguintes dispositivos móveis/sistema operacional:

- Pocket PC / Windows Mobile 2003 SE
- Pocket PC / Windows Mobile 5.0
- Smart Phone / Windows Mobile 2003 SE
- Smart Phone / Windows Mobile 5.0

Através do "*Device Emulator Manager*" (gerenciador de imagens), carregamos as imagens dos sistemas operacionais dos dispositivos, sendo possível simular o fato do dispositivo estar ou não em sua base (*craddle*). A documentação do emulador afirma que este suporta os mesmos binários utilizados pelos equipamentos reais, tanto quanto a arquitetura do processador ARM.

Foi possível fazer a comunicação do emulador com o Microsoft ActiveSync, software de sincronização de dados entre o PocketPC e o PC.

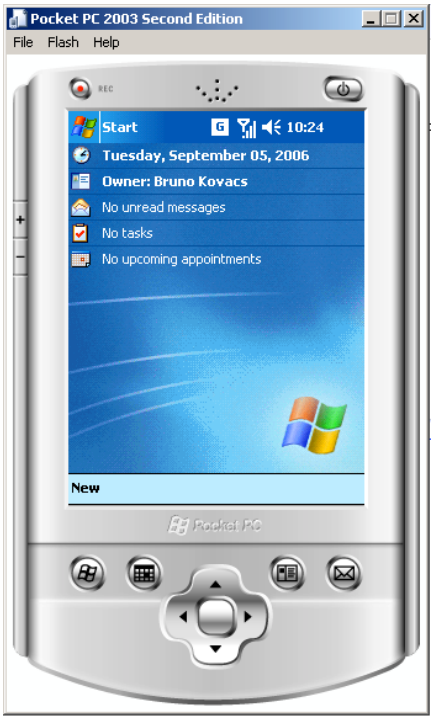


Figura 11: Emulação do Windows Mobile 2003 SE em PocketPC

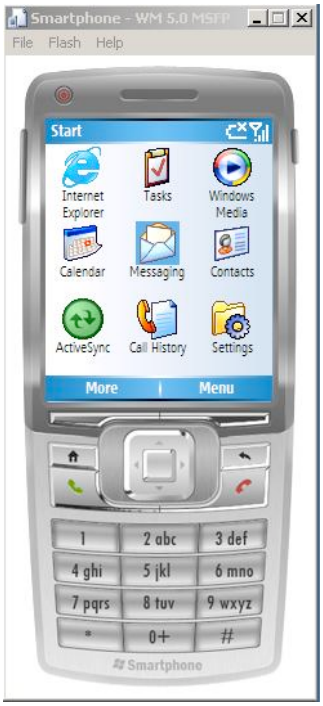


Figura 12: Emulação do Windows Mobile 2003 SE em SmartPhone

5.1.2. Descrição do ambiente de testes com dispositivos físicos

Os testes práticos com dispositivos físicos foram realizados no Laboratório de Colaboração Avançada (LAC/Laboratory of Advanced Collaboration) da Pontifícia Universidade Católica do Rio de Janeiro (PUC-RIO). O ambiente foi composto pelos seguintes modelos de PocketPC e mais um PC com acesso à Internet:

- HP IPaq HX2490b - Microsoft Windows Mobile 5.0 (Windows CE 5.0) – Interfaces de rede Wi-Fi e Bluetooth

- HP IPaq H5450 - Microsoft Windows Mobile 2003 (Windows CE 4.2) - Interfaces de rede Wi-Fi e Bluetooth

5.1.3. Vantagens e desvantagens quanto aos ambientes

Os testes foram realizados nos dois ambientes citados anteriormente devido à presença de vantagens e desvantagens oriundas de cada um.

O ambiente de testes com emuladores nos trouxe a facilidade de trabalhar com aplicações desenvolvidas para os sistemas operacionais Windows Mobile 2003 e 5.0 em arquitetura ARM, em nossas próprias máquinas pessoais. Estas aplicações foram encontradas na Internet e pôde-se verificar a compatibilidade e reconhecimento pelos mesmos. Além disso, permitiu o manuseio parcial destas aplicações, sendo possível descobrir como funcionavam antes de testá-las em dispositivos físicos do laboratório. Os testes com emuladores nos permiram além de tudo, conhecer melhor o próprio sistema operacional estudado, apesar das limitações de performance ocasionadas devido aos recursos da máquina hospedeira.

Os testes com dispositivos reais foram mais ilustrativos, pois representavam a realidade ou algo muito similar ao ambiente utilizado por um atacante. Os testes com dispositivos reais possibilitaram as aplicações a executarem de forma mais performática do que nos emuladores, mas a grande vantagem era a facilidade de uso das interfaces de rede 802.11 e Bluetooth nativamente.

5.2. Discussão sobre metodologia e critérios de avaliação

As vulnerabilidades testadas serão apresentadas individualmente, com a sua respectiva descrição e resultados obtidos na próxima seção. Serão avaliadas aquelas que forem possíveis dentro do espaço de tempo e recusos disponíveis para a realização deste trabalho.

Procedimento dos testes

Os procedimentos utilizados podem ser comparados a ataques reais, pois fizeram uso de aplicações conhecidas e utilizadas por atacantes, que podem ser obtidas facilmente na Internet. Na verdade, testes em laboratório podem apresentar poder de exploração ainda maior do que ataques reais, pois o ambiente pode ser ajustado, aumentando ou diminuindo a dificuldade para se obter sucesso. Um atacante real, muitas vezes, precisa buscar meios alternativos para facilitar a sua execução, através de técnicas como, por exemplo, engenharia social.

Critérios de avaliação

O critério de sucesso utilizado nos testes foi a reprodução de experimentos com o uso de aplicações desenvolvidas pela comunidade de segurança mundial. Cada teste foi feito individualmente, estipulando um limite de tempo e número de tentativas para casos falhos. Estes variaram para cada situação até que comprovassem funcionamento ou falha.

5.3. Testes com emuladores

Requisitos de sistema operacional para uso dos emuladores:

- Windows Server 2003 com Service Pack 1
- Windows XP

Teste: Instalação da ferramenta de varredura de redes Wi-fi Mini-Stumbler

Descrição: Uma das aplicações mais conhecidas para varredura de redes 802.11 é chamada NetworkStumbler. Esta é capaz de medir o sinal de cada rede detectada, indicar se usa criptografia ou não e prover informações sobre o hardware identificado. No entanto, uma versão específica para PocketPCs foi criada, com o nome Mini-Stumbler.

Restrições para funcionamento: o emulador preferencialmente deve estar configurado para usar a interface Wi-Fi do PC onde está sendo executado.

Resultados: A aplicação foi instalada com sucesso, mas não foi possível utilizar suas funções principais mesmo com PC local possuindo interface de rede sem fio. A aplicação só suporta uma quantidade limitada de equipamentos, listados em: http://www.stumbler.net/compat/.

Teste: Captura de tráfego da rede com a ferramenta VxSniffer

Descrição: O VxSniffer é uma aplicação para coleta de tráfego de rede, que funciona deixando a interface em modo promíscuo ou somente observando o tráfego originado/destinado à interface local. Assim, caso a rede não faça uso de criptografia, é possível observar o que os usuários ao redor estão acessando em tempo real, coletar credenciais de contas pessoais e outras informações sigilosas. É possível determinar qual a interface de rede do dispositivo que será usada para esta função.

Restrições para funcionamento: uso do software ActiveSync para sincronização de arquivos e instalação da ferramenta.

Resultados: A aplicação foi instalada com sucesso e foi possível coletar tráfego da interface local da máquina hospedeira do emulador. No entanto, como esta está ligada a um switch, somente o tráfego de broadcast ou local pôde ser observado.

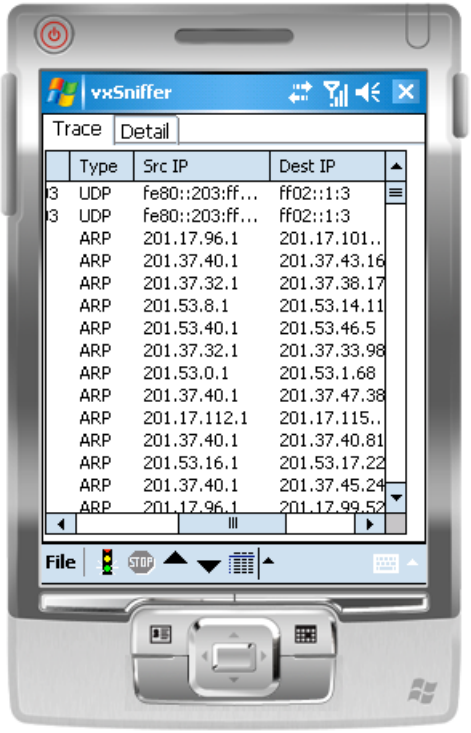


Figura 13: VxSniffer coletou tráfego da interface local

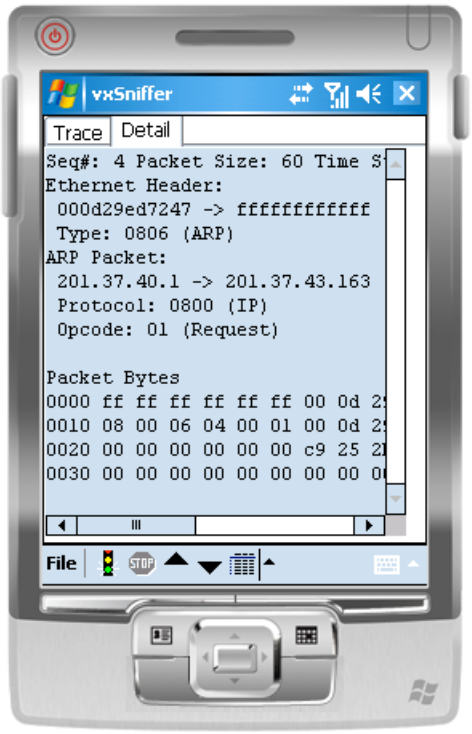

vxSniffer
Trace
Detail
Seq#: 4 Packet Size: 60 Time S
Ethernet Header:
000d29ed7247 -> ffffffffffff
Type: 0806 (ARP)
ARP Packet:
201.37.40.1 -> 201.37.43.163
Protocol: 0800 (IP)
Opcode: 01 (Request)
Packet Bytes
0000 ff ff ff ff ff ff 00 0d 2
0010 08 00 06 04 00 01 00 0d 2
0020 00 00 00 00 00 00 c9 25 2
0030 00 00 00 00 00 00 00 00 0
File

Figura 14: Detalhes de uma requisição do protocolo ARP

Teste: Uso de ferramenta de análise forense (*dumper*) para coleta de todas as informações do dispositivo para posterior análise.

Descrição: Foi utilizada a ferramenta PDA Seizure, uma das mais conhecidas para análise forense de dispositivos móveis.

Restrições para funcionamento: A aplicação suporta somente os seguintes modelos da série IPAQ: H 1940, H 3630, H 3670, H 3760, H4155, HX2110, HX4705, RX1955, RX3115, RX3715, RZ1715. Mais informações: http://www.paraben-forensics.com/cell_models.html.

Resultados: Não foi possível utilizar esta ferramenta com o emulador, pois esta só é compatível com uma versão do ActiveSync inferior à única versão compatível com o emulador.

5.4. Testes locais

Teste: Execução de aplicações por *Auto-run*

Descrição: Um arquivo chamado "autorun.exe" em uma pasta chamada "2577" na raiz de um cartão de memória (considerando que o dispositivo trabalha com processador ARM) é copiado para a pasta local do Windows Móbile e executado automaticamente caso detectado. Se o arquivo for algum tipo de código malicioso, é executado sem a intervenção do usuário. Para realizar este teste, foi usado um cartão de memória do tipo SD (Secure Digital Card), utilizando binários obtidos através de fontes na Internet, específicos para executarem um soft reset no dispositivo, ou seja, reiniciá-lo independente do estado em que esteja operando.

Restrições para funcionamento: necessidade de um cartão de memória e manuseio direto do equipamento.

Resultados: Foi comprovado que o sistema de auto-run funciona nas condições descritas a cima. Foi observado instanteneamente o reiniciar do sistema assim que o SD Card foi inserido.

Teste: Infecção com porta dos fundos (*backdoor*)

Descrição: Teste de manipulação de binários existentes, transformando-os em uma porta dos fundos. Foram realizados testes com um servidor FTP e um servidor de terminal remoto.

Restrições para funcionamento: para ser acessado, o dispositivo deve estar acessível via rede. Em nossos testes, o acessamos através da Internet pois existia um endereço IP público associado ao IP interno do dispositivo através de NAT (network address translation).

Resultados: O servidor de FTP pôde ser instalado e testado (acessamos o PocketPC através da Internet), mas apesar de utilizarmos a ferramenta indicada para edição do binário, não foi possível excluir a rotina de exibição do ícone da aplicação (único identificador de sua presença no sistema). Quanto à aplicação de terminal remoto, foi possível testá-la com sucesso, acessar o dispositivo através da Internet mas, da mesma forma, não editamos o binário para torná-lo invisível para o usuário. A seguir, as telas obtidas:

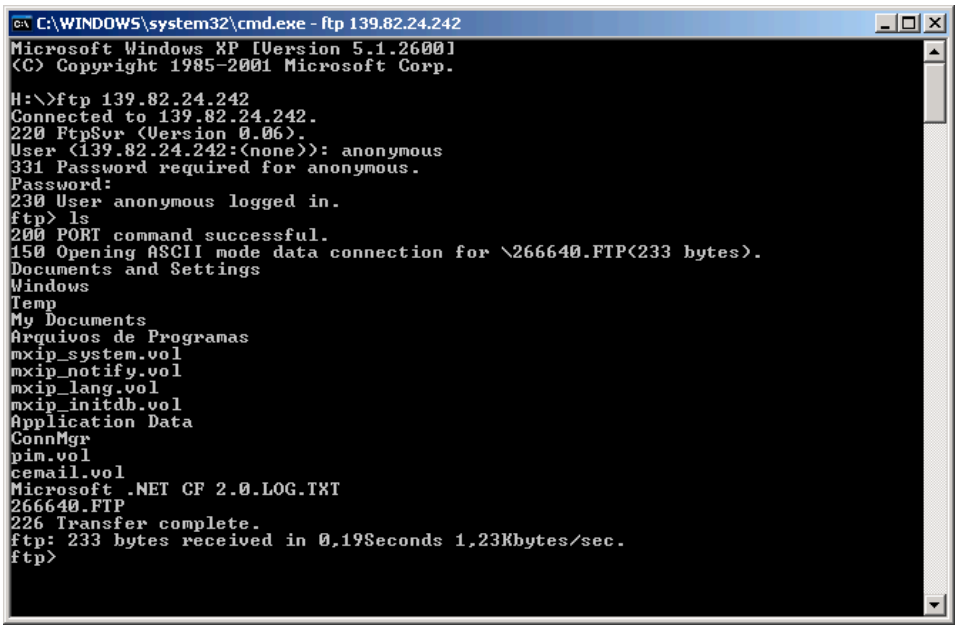


Figura 15: Acesso via FTP através da Internet ao PocketPC e exibição dos arquivos locais.

Figura 16: Autenticação com senha para acesso remoto (Através da aplicação VirtualCE)

Figura 17: Controle remoto do PocketPC via Internet

Figura 18: Controle remoto do PocketPC via Internet

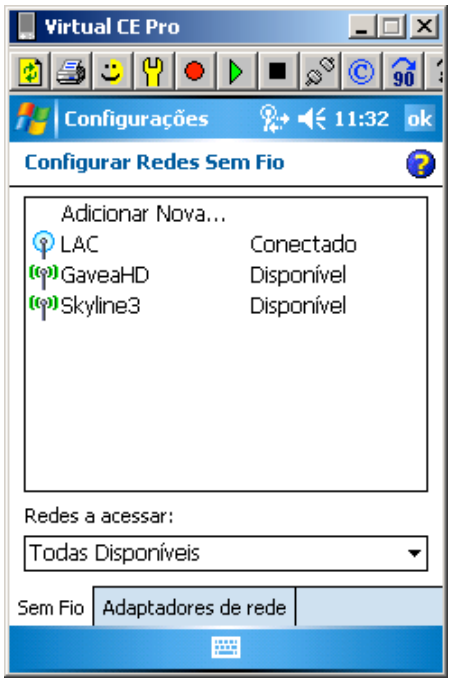


Figura 19: Controle remoto do PocketPC via Internet

Teste: Uso de ferramenta de análise forense (*dumper*) para coleta de todas as informações do dispositivo para posterior análise.

Descrição: Foi utilizada a ferramenta "PDA Seizure", uma das mais conhecidas para análise forense de dispositivos móveis.

Restrições para funcionamento: A aplicação suporta somente os seguintes modelos da série IPAQ: H 1940, H 3630, H 3670, H 3760, H4155, HX2110, HX4705, RX1955, RX3115, RX3715, RZ1715. Mais informações: http://www.paraben-forensics.com/cell_models.html.

Resultados: A versão do ActiveSync exigida pela aplicação é a 3.7.0 ou 3.7.1. Removemos a versão 4.0 e tentamos instalar uma das versões requisitadas, mas não obtivemos sucesso devido à incompatibilidades com o Windows XP. A aplicação pôde ser iniciada, mas ao tentar-se adquirir a imagem do PDA, a comunicação não foi estabelecida com sucesso. Abaixo, apresentamos uma tela que mostra as informações que poderiam ter sido obtidas:

5.5. Testes com Bluetooth

Teste: Roubo de informações (agenda telefônica, calendário, fotos, etc - *Bluesnarfing*) e envio de mensagens inoportunas (*Bluejacking*).

Descrição: As técnicas de *Bluesnarfing* e *Bluejacking* foram implementadas na aplicação BTCrawler, suportada pelo Windows Mobile 2003/5.0.

Restrições para funcionamento: nem todos os dispositivos com suporte a Bluetooth são vulneráveis a estes ataques. Segundo o desenvolvedor da aplicação, os seguintes são:

Nokia 6310, 6310i (até a versão de firmware 5.51), Nokia 8910, 8910i, SE T610 FW:R1A081, SE T630 FW:R4C003, SE T68i FW:R2B025, SE Z600 FW:R2E004, SE Z1010.

Resultados: Foi possível instalar a aplicação, mas apesar da comunicação via Bluetooth dos dispositivos estar operando normalmente, a aplicação foi incapaz de detectar telefones celulares com Bluetooth habilitados ou outros PocketPCs. A seguir, mostramos as telas de configuração do dispositivo para que ficasse no modo visível e da aplicação btCrawler, a mais indicada para este tipo de teste.

Obs.: A função de *Bluesnarfing* da aplicação precisou ser habilitada através da edição do registro do PocketPC (feita com uso de aplicação terceira).

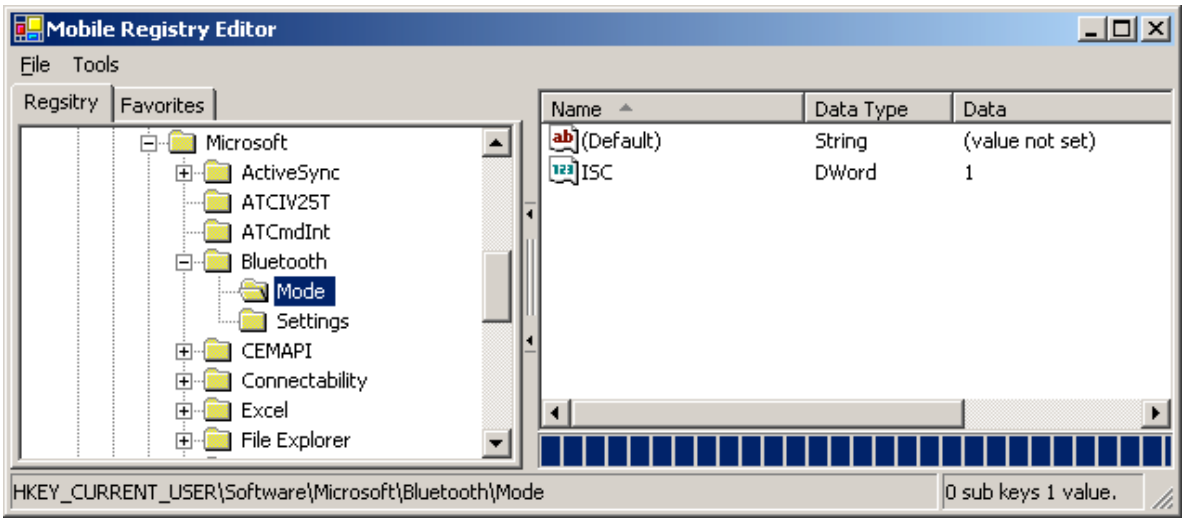


Figura 20: Editando o registro do Windows Mobile através da aplicação "Mobile Registry Editor"

Figura 21: Habilitando a interface Bluetooth do dispositivo

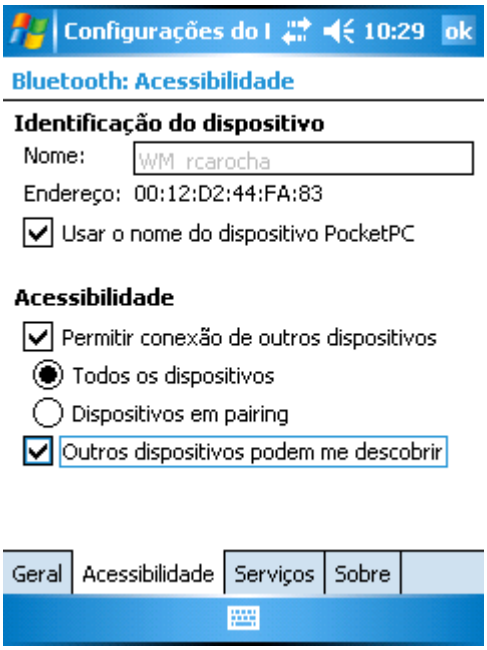


Figura 22: Configurando a interface Bluetooth do dispositivo para estar visível

Figura 23: Aplicação btCrawler com função de bluesnarfing habilitada via edição de registro.

Procedimento para habilitar a função de bluesnarfing:

1. Criar a seguinte chave de registro:
   \HKCU\Software\Microsoft\Bluetooth\Mode

2. Criar a seguinte DWORD:

Nome: ISC

Valor: 1

5.6. Testes com IEEE 802.11

Teste: Instalação da ferramenta de varredura de redes Wi-fi Mini-Stumbler

Descrição: Uma das aplicações mais conhecidas para varredura de redes 802.11 é chamada NetworkStumbler. Esta é capaz de medir o sinal de cada rede detectada, indicar se usa criptografia ou não e prover informações sobre o hardware identificado. No entanto, uma versão específica para PocketPCs foi criada, com o nome Mini-Stumbler.

Restrições para funcionamento: a interface de rede sem fio deve ser identificada pelo dispositivo.

Resultados: A aplicação foi instalada com sucesso, mas não foi possível utilizar suas funções pois a interface Wi-Fi dos dispositivos disponíveis para teste não foram identificadas pela aplicação.

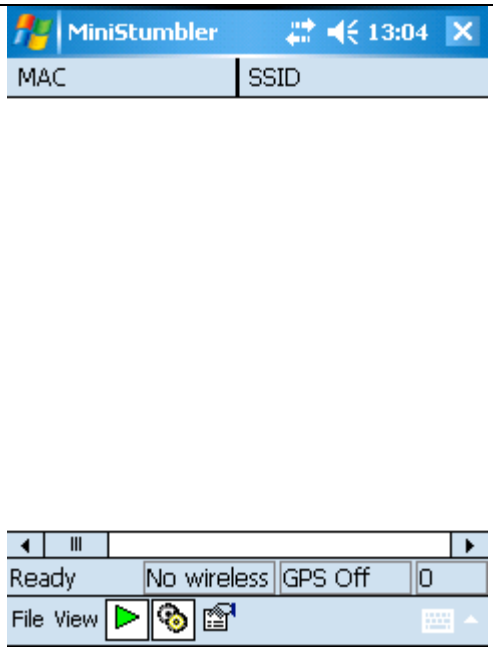


Figura 24: Mini-stumbler não reconheceu a interface de rede sem fio.

Teste: Captura de tráfego da rede com a ferramenta VxSniffer

Descrição: O VxSniffer é uma aplicação para coleta de tráfego de rede, que funciona deixando a interface em modo promíscuo ou somente observando o tráfego originado/destinado à interface local. Assim, caso a rede não faça uso de criptografia, é possível observar o que os usuários ao redor estão acessando em tempo real, coletar credenciais de contas pessoais e outras informações sigilosas. É possível determinar qual a interface de rede do dispositivo que será usada para esta função.

Restrições para funcionamento: para coletar tráfego de outras estações, a interface de rede deve suportar o modo promíscuo.

Resultados: A aplicação foi instalada com sucesso, mas só foi possível varrer o tráfego de rede originado ou destinado ao dispositivo móvel, pois sua interface Wi-fi não permite ser configurada para modo promíscuo. A seguir, apresentamos as telas capturadas com detalhes do tráfego:

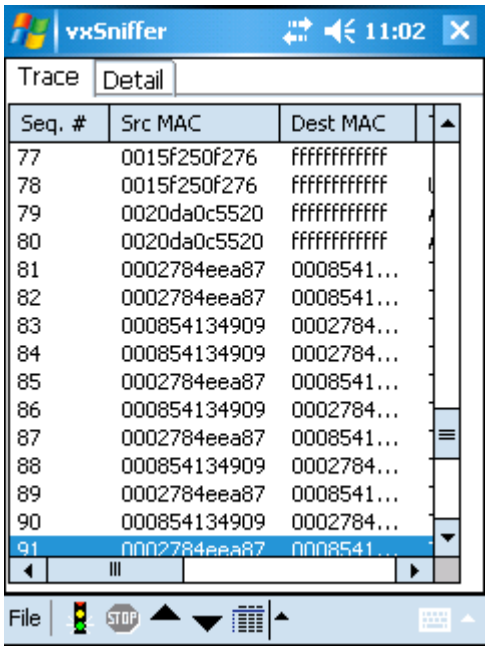


Figura 25: Captura de tráfego da rede 802.11 do LAC

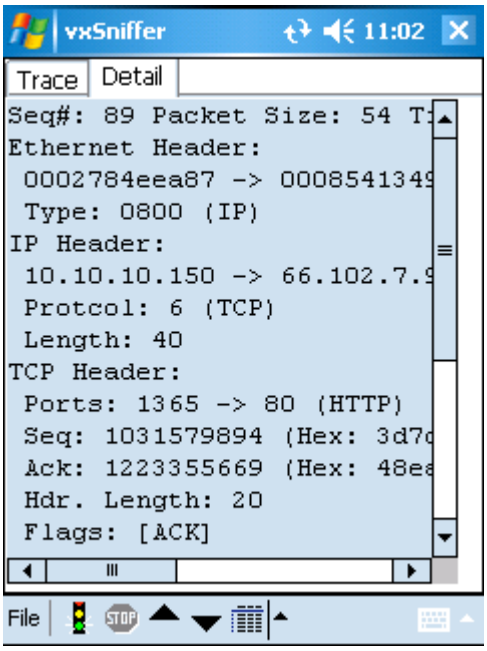
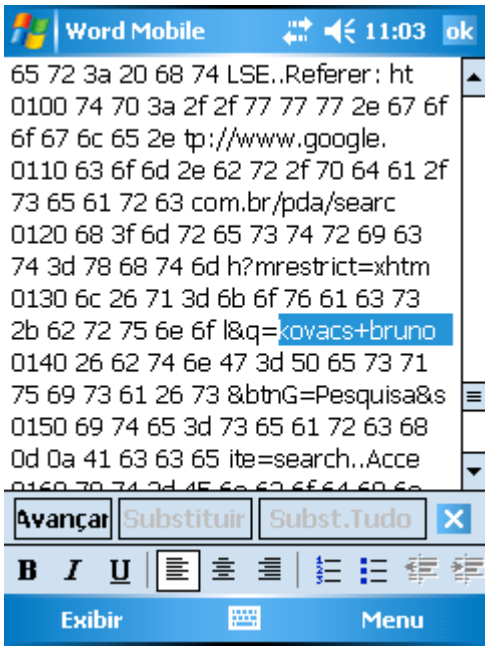


Figura 26: Detalhes do segmento TCP capturado



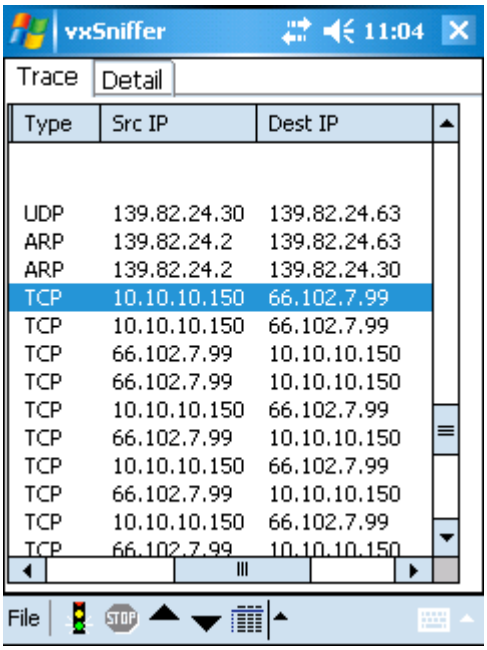


Figura 27: Análise do conteúdo capturado. Pode-se visualizar o conteúdo das requisições.

Figura 28: Exibição dos pacotes capturados.

Teste: Quebra da chave criptográfica WEP (*Wired Equivalent Privacy*).

Descrição: Existem diversas implementações para atacar o algoritmo criptográfico WEP, tanto em suas versões de chave de 40 ou 104 bits. No entanto, a única disponível para Windows Mobile foi criada pela empresa E-Eye Security, sendo chamada de Retina Wifi Scanner.

Restrições para funcionamento: apesar do manual afirmar que a ferramenta funciona em PocketPCs, não tivemos sucesso ao utilizá-la pois o sistema exibiu um erro afirmando que não suporta a aplicação.

Resultados: Infelizmente a aplicação não foi reconhecida como válida quando executada no PocketPC. Fizemos os testes em Windows XP, sendo capazes de identificar redes 802.11, medindo seu sinal e identificando caracterísiticas dos Access Points, mas não foi possível quebrar a chave WEP. A "resposta" da chave foi inserida ao dicionário de ataque, mas a aplicação retornou erros afirmando que não conseguiu iniciar o ataque. Tivemos uma séria impressão de que esta aplicação é de caráter experimental e não possuir todos os recursos funcionando corretamente. Um indício disso é a sua gratuidade.

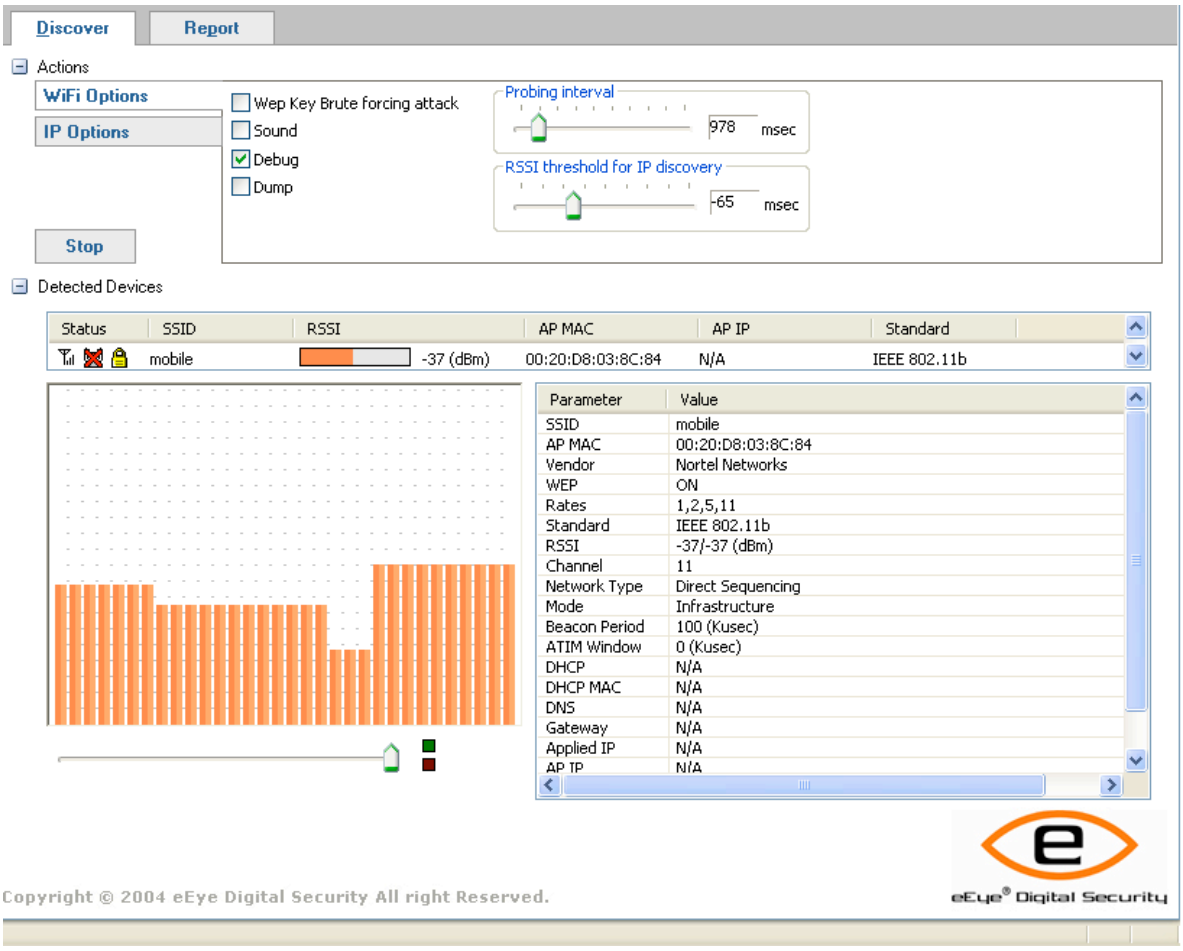


Figura 29: Ferramenta E-eye WiFi Scanner identificou uma rede 802.11 com WEP habilitado

6. Conclusão

Este trabalho ilustrou ameaças de segurança a dispositivos de computação móvel, abrangendo os principais sistemas operacionais e tecnologias de rede sem fio do mercado. Percebe-se que ainda não há uma consciência dos perigos existentes por quase a totalidade dos usuários destes dispositivos. Muitos deles são executivos e apesar de carregarem consigo informações sigilosas, que nunca deveriam cair em mãos erradas, não se preocupam com este tipo de problema.

Existe uma tendência natural para a evolução das ameaças que cincurdam dispositivos móveis, à medida que seu uso se torne mais popular. Algumas empresas já estão se preparando e desenvolvendo softwares para aumentar o nível de segurança de PDAs, como por exemplo

sistemas de criptografia de dados e firewalls pessoais. O poder de disseminação das ameaças se tornará cada vez maior, causando grandes prejuízos aos não preparados.

Cabe aos desenvolvedores de software, buscarem melhorar a qualidade de seus produtos para que menos falhas de segurança ocorram, e também aos usuários de PDAs a reclamarem quando estão insatisfeitos com a qualidade de determinada solução. A indústria de tecnologia está sempre sob pressão, e só abre espaço para aspectos que não são vistos como lucrativos quando o mercado exige.

No entanto, existe um movimento presente buscando aumentar a consciência quanto ameaças de segurança de modo geral e evitar que aconteça novamente nos PDAs o que acontece com estaçoes de trabalho e máquinas pessoais, infectadas com virus e worms, que já causaram prejuízos enormes a diversas instituições.

Os testes realizados neste estudo apresentaram vulnerabilidades de grande impacto, mas que atualmente já podem ser remediadas com mecanismos substitutos. Por exemplo, a quebra de chaves WEP estimulou fortemente o estudo de novas soluções de criptografia, dando origem ao WPA, considerado seguro atualmente.

Técnicas como *BlueSnarfing*, que dá margem à captura de informações sigilosas via bluetooth, não afetam dispositivos recém-fabricados, pois já receberam correções de segurança para remediar esta vulnerabilidade. No entanto, já se pode notar a tendência de que usuários de dispositivos móveis estejam cada vez mais conectados à Internet, que dependam cada vez mais destes recursos e que códigos maliciosos serão criados para explorar este fato. A exploração poderá se dar de inúmeros maneiras, por exemplo, capturando senhas de banco e credenciais de aplicações (como correio eletrônico), e algumas ainda mais preocupantes, como a identificação da localização física da vítima e contaminação dos dispositivos por mecanismos de espionagem.

Infelizmente, os dispositivos móveis mais comuns de mercado ainda são muito heterogêneos em termos de configuração de hardware, drivers específicos e pode-se dizer que até mesmo em termos de sistemas operacionais. Este fato foi de certa forma uma barreira para nossos testes, pois muitas das aplicações disponíveis hoje para provas de conceito suportam apenas alguns dispositivos, com interfaces de rede específicas, o que nos impediu de verificar o funcionamento de muitas destas.

Pode-se dizer que o número de ameaças de segurança a dispositivos de computação móvel existentes atualmente é proporcional à quantidade de usuários e à maturidade dos mecanismos de proteção. Isso significa que muito ainda irá evoluir neste cenário, e portanto, deve-se estar preparado para o aparecimento de ameaças inovadoras, com grande poder de destruição e roubo de informações em massa.

7. Referências Bibliográficas

[1] BLUEJACKQ - URL: www.bluejackq.com

[2] WIKIPEDIA – "BLUEJACKING (ROUBO DE DADOS)"
URL: http://pt.wikipedia.org/wiki/Bluetooth#Bluejacking_.28Roubo_de_dados.29

[3] WIKIPEDIA – "WEP" - URL: http://pt.wikipedia.org/wiki/WEP

[4] WIKIPEDIA – "WPA" - URL: http://pt.wikipedia.org/wiki/WPA

[5] WIKIPEDIA – "IEEE 802.11" – URL: http://pt.wikipedia.org/wiki/ieee_802.11

[6] NIKITA BORISOV, IAN GOLDBERG, E DAVID WAGNER; "SECURITY OF THE WEP ALGORITHM"
URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[7] SETH FOGIE, INSECURE MAGAZINE, EDIÇÃO 1.3, "PDA ATTACKS: PALM SIZED DEVICES - PC SIZED THREATS" URL: www.insecuremag.com.

[8] CYRUS PEIKARI, INSECURE MAGAZINE, EDIÇÃO 1.4, "PDA ATTACKS, PART 2: AIRBORNE VIRUSES - EVOLUTION OF THE LATEST THREATS".

[9] http://www.noconname.org/ponentes/olliewhitehouse.htm

[10] SONY ERICSSON - URL: http://www.sonyericsson.com

[11] MOTOROLA - URL: http://www.motorola.com.br

[12] LINUX – URL: http://br-linux.org/

[13] INTEL - URL: http://www.intel.com

[14] IBM - URL: http://www.motorola.com.br

[15] TOSHIBA - URL: http://www.toshiba.com

[16] MICROSOFT - URL: http://www.microsoft.com

[17] TOYOTA - URL: http://www.toyota.com

[18] BMW - URL: http://www.bmw.com

[19] LEXUS - URL: http://www.lexus.com

[20] ERICSSON - URL: http://www.ericsson.com

[21] APPLE - URL: http://www.apple.com

[22] DELL - URL: http://www.dell.com

[23] HP - URL: http://www.hp.com

[24] 3COM - URL: http://www.ecom.com.br

[25] LUCENT - URL: http://www.lucent.com

[26] ADAM LAURIE - URL: http://trifinite.org/trifinite_group_adam.html

[27] NOKIA – URL: http://www.nokia.com

[28] IDC - URL: http://www.idclatin.com/brasil/

[29] PARABEN - URL: http://www.paraben.com

[30] HOME OF BTCRAWLER - A BLUETOOTH DIAGNOSTIC TOOL – URL: http://www.silentservices.de/btCrawler.html

[31] RED FANG BLUETOOTH TOOL
http://www.netstumbler.com/2003/08/18/software_tool_steals_data_via_bluetooth/